Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9200 Switches)

First Published: 2019-07-31

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

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: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 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 I **Cisco SD-Access** 13

CHAPTER 2 **Cisco SD-Access Commands** 15

broadcast-underlay 17

database-mapping 18

dynamic-eid 20

eid-record-provider 21
eid-record-subscriber 22
eid-table 23
encapsulation 25
etr 26
etr map-server 27
extranet 28
instance-id 29
ip pim lisp core-group-range 30
ip pim lisp transport multicast 31
ip pim rp-address 32
ip pim sparse mode 33
ipv4 multicast multitopology 34
ip pim ssm 35
itr 36
itr map-resolver 37
locator default-set 38
locator-set 39
map-cache 40
map-cache extranet 41
prefix-list 42
route-import database 43
service 45
show lisp instance-id ipv4 database 46
show lisp instance-id ipv6 database 48
show lisp instance-id ipv4 map-cache 49
show lisp instance-id ipv6 map-cache 55
show lisp instance-id ipv4 server 57
show lisp instance-id ipv6 server 59
show lisp instance-id ipv4 statistics 60
show lisp instance-id ipv6 statistics 61
show lisp prefix-list 62
show lisp session 63
use-petr 64

PART II Cisco TrustSec 67

CHAPTER 3 Cisco TrustSec Commands 69

cts authorization list 71

cts change-password 72

cts credentials 73

cts refresh 75

cts rekey 77

cts role-based enforcement 78

cts role-based l2-vrf 79

cts role-based monitor 81

cts role-based permissions 82

cts role-based sgt-caching 84

cts role-based sgt-map 85

cts sxp connection peer 87

cts sxp default password 90

cts sxp default source-ip 92

cts sxp filter-enable 94

cts sxp filter-group 95

cts sxp filter-list 97

cts sxp log binding-changes 99

cts sxp reconciliation period 100

cts sxp retry period 101

propagate sgt (cts manual) 102

sap mode-list (cts manual) 104

show cts credentials 106

show cts interface 107

show cts role-based counters 109

show cts role-based permissions 111

show cts server-list 113

show cts sxp 115

show platform hardware fed switch active fwd-asic resource tcam utilization 118

show platform hardware fed switch active sgacl resource usage 120

show platform software classification switch active F0 class-group-manager class-group client acl all 121
show platform software cts forwarding-manager switch active F0 port 122
show platform software cts forwarding-manager switch active F0 126
show platform software cts forwarding-manager switch active F0 permissions 127
show platform software fed switch active acl counters hardware | inc SGACL 129
show platform software fed switch active acl usage 130
show platform software fed switch active ifm mappings 131
show platform software fed switch active ip route 133
show platform software fed switch active sgacl detail 135
show platform software fed switch active sgacl port 136
show platform software fed switch active sgacl vlan 138
show platform software status control-processor brief 139
show monitor capture <name> buffer 140

PART III **Interface and Hardware Components** 141

CHAPTER 4 **Interface and Hardware Commands** 143

bluetooth pin 146
clear coap database 147
clear macro auto configuration 148
coap endpoint (coap-proxy configuration) 149
debug coap 150
device classifier 151
debug ilpower 152
debug interface 153
debug lldp packets 154
debug platform poe 155
debug platform software fed switch active punt packet-capture start 156
duplex 157
errdisable detect cause 159
errdisable recovery cause 161
errdisable recovery cause 163
interface 165

interface range 167
ip mtu 169
ipv6 mtu 170
list (coap-proxy configuration) 171
lldp (interface configuration) 172
logging event power-inline-status 174
macro 175
macro auto 178
macro auto apply (Cisco IOS shell scripting capability) 181
macro auto config (Cisco IOS shell scripting capability) 183
macro auto control 184
macro auto execute 186
macro auto global control 193
macro auto global processing 195
macro auto mac-address-group 196
macro auto processing 198
macro auto sticky 199
macro auto trigger 200
macro description 201
macro global 202
macro global description 204
max-endpoints (coap-proxy configuration) 205
mdix auto 206
network-policy 207
network-policy profile (global configuration) 208
port-dtls (coap-proxy configuration) 209
port-unsecure (coap-proxy configuration) 210
power inline 211
power inline police 214
power supply 216
resource directory (coap-proxy configuration) 218
security (coap-proxy configuration) 219
shell trigger 220
show beacon all 221

show coap dtls endpoints 222
show coap endpoints 223
show coap globals 224
show coap resources 225
show coap stats 226
show coap version 227
show device classifier attached 228
show device classifier clients 230
show device classifier profile type 231
show environment 234
show errdisable detect 236
show errdisable recovery 238
show ip interface 239
show interfaces 244
show interfaces counters 250
show interfaces switchport 252
show interfaces transceiver 254
show macro auto 258
show memory platform 261
show module 264
show network-policy profile 265
show parser macro 266
show platform hardware bluetooth 269
show platform hardware fed switch forward interface 270
show platform resources 273
show platform software audit 274
show platform software fed switch punt cpuq rates 278
show platform software fed switch punt packet-capture display 280
show platform software fed switch punt rates interfaces 282
show platform software ilpower 285
show platform software memory 287
show platform software process list 293
show platform software process memory 297
show platform software process slot switch 300

show platform software status control-processor 302
show platform software thread list 305
show processes cpu platform 307
show processes cpu platform history 310
show processes cpu platform monitor 313
show processes memory 315
show processes memory platform 318
show processes platform 322
show shell 325
show system mtu 328
show tech-support 329
show tech-support bgp 331
show tech-support diagnostic 334
speed 336
start (coap-proxy configuration) 338
stop (coap-proxy configuration) 339
switchport block 340
system mtu 341
transport (coap-proxy configuration) 342
voice-signaling vlan (network-policy configuration) 343
voice vlan (network-policy configuration) 345

PART IV IP Addressing Services 347

CHAPTER 5 IP Addressing Services Commands 349
clear ipv6 access-list 353
clear ipv6 dhcp 354
clear ipv6 dhcp binding 355
clear ipv6 dhcp client 356
clear ipv6 dhcp conflict 357
clear ipv6 dhcp relay binding 358
clear ipv6 eigrp 359
clear ipv6 mfib counters 360
clear ipv6 mld counters 361

clear ipv6 mld traffic 362
clear ipv6 mtu 363
clear ipv6 multicast aaa authorization 364
clear ipv6 nd destination 365
clear ipv6 nd on-link prefix 366
clear ipv6 nd router 367
clear ipv6 neighbors 368
clear ipv6 ospf 370
clear ipv6 ospf counters 371
clear ipv6 ospf events 373
clear ipv6 pim reset 374
clear ipv6 pim topology 375
clear ipv6 pim traffic 376
clear ipv6 prefix-list 377
clear ipv6 rip 378
clear ipv6 route 379
clear ipv6 spd 380
fhrp delay 381
fhrp version vrrp v3 382
ip address dhcp 383
ip address pool (DHCP) 386
ip address 387
ip unnumbered 389
ip wccp 391
ipv6 access-list 396
ipv6 address-validate 399
ipv6 cef 400
ipv6 cef accounting 402
ipv6 cef distributed 404
ipv6 cef load-sharing algorithm 406
ipv6 cef optimize neighbor resolution 407
ipv6 destination-guard policy 408
ipv6 dhcp-relay bulk-lease 409
ipv6 dhcp-relay option vpn 410

ipv6 dhcp-relay source-interface 411
ipv6 dhcp binding track ppp 412
ipv6 dhcp database 413
ipv6 dhcp iana-route-add 415
ipv6 dhcp iapd-route-add 416
ipv6 dhcp-ldra 417
ipv6 dhcp ping packets 418
ipv6 dhcp pool 419
ipv6 dhcp server vrf enable 421
ipv6 flow monitor 422
ipv6 general-prefix 423
ipv6 local policy route-map 425
ipv6 local pool 427
ipv6 mld snooping (global) 429
ipv6 mld ssm-map enable 430
ipv6 mld state-limit 431
ipv6 multicast-routing 432
ipv6 multicast group-range 433
ipv6 multicast pim-passive-enable 435
ipv6 nd cache expire 436
ipv6 nd cache interface-limit (global) 437
ipv6 nd host mode strict 438
ipv6 nd na glean 439
ipv6 nd ns-interval 440
ipv6 nd nud retry 441
ipv6 nd reachable-time 443
ipv6 nd resolution data limit 444
ipv6 nd route-owner 445
ipv6 neighbor 446
ipv6 ospf name-lookup 448
ipv6 pim 449
ipv6 pim accept-register 450
ipv6 pim allow-rp 451
ipv6 pim neighbor-filter list 452

ipv6 pim rp-address 453
ipv6 pim rp embedded 456
ipv6 pim spt-threshold infinity 457
ipv6 prefix-list 458
ipv6 source-guard attach-policy 461
ipv6 source-route 462
ipv6 spd mode 464
ipv6 spd queue max-threshold 465
ipv6 traffic interface-statistics 466
ipv6 unicast-routing 467
key chain 468
key-string (authentication) 469
key 470
show ip ports all 472
show ipv6 access-list 474
show ipv6 destination-guard policy 476
show ipv6 dhcp 477
show ipv6 dhcp binding 478
show ipv6 dhcp conflict 481
show ipv6 dhcp database 482
show ipv6 dhcp guard policy 484
show ipv6 dhcp interface 486
show ipv6 dhcp relay binding 488
show ipv6 eigrp events 490
show ipv6 eigrp interfaces 492
show ipv6 eigrp topology 494
show ipv6 eigrp traffic 496
show ipv6 general-prefix 498
show ipv6 interface 499
show ipv6 mfib 507
show ipv6 mld groups 513
show ipv6 mld interface 516
show ipv6 mld snooping 518
show ipv6 mld ssm-map 520

show ipv6 mld traffic 522
show ipv6 mrib client 524
show ipv6 mrib route 526
show ipv6 mroute 528
show ipv6 mtu 532
show ipv6 nd destination 534
show ipv6 nd on-link prefix 535
show ipv6 neighbors 536
show ipv6 ospf 540
show ipv6 ospf border-routers 544
show ipv6 ospf event 546
show ipv6 ospf graceful-restart 549
show ipv6 ospf interface 551
show ipv6 ospf request-list 556
show ipv6 ospf retransmission-list 558
show ipv6 ospf statistics 560
show ipv6 ospf summary-prefix 562
show ipv6 ospf timers rate-limit 563
show ipv6 ospf traffic 564
show ipv6 ospf virtual-links 568
show ipv6 pim anycast-RP 570
show ipv6 pim bsr 571
show ipv6 pim df 573
show ipv6 pim group-map 575
show ipv6 pim interface 577
show ipv6 pim join-prune statistic 579
show ipv6 pim limit 580
show ipv6 pim neighbor 581
show ipv6 pim range-list 583
show ipv6 pim topology 585
show ipv6 pim traffic 587
show ipv6 pim tunnel 589
show ipv6 policy 591
show ipv6 prefix-list 592

show ipv6 protocols 594
show ipv6 rip 596
show ipv6 routers 601
show ipv6 rpf 604
show ipv6 source-guard policy 606
show ipv6 spd 607
show ipv6 static 608
show ipv6 traffic 612
show key chain 615
show track 616
track 618
vrrp 620
vrrp description 621
vrrp preempt 622
vrrp priority 623
vrrp timers advertise 624
vrrs leader 626

PART V IP Multicast Routing 627

CHAPTER 6 IP Multicast Routing Commands 629
clear ip mfib counters 631
clear ip mroute 632
clear ip pim snooping vlan 633
ip igmp filter 634
ip igmp max-groups 635
ip igmp profile 637
ip igmp snooping 638
ip igmp snooping last-member-query-count 639
ip igmp snooping querier 641
ip igmp snooping report-suppression 643
ip igmp snooping vlan mrouter 644
ip igmp snooping vlan static 645
ip multicast auto-enable 646

ip multicast-routing 647
ip pim accept-register 648
ip pim bsr-candidate 649
ip pim rp-candidate 651
ip pim send-rp-announce 652
ip pim snooping 654
ip pim snooping dr-flood 655
ip pim snooping vlan 656
ip pim spt-threshold 657
match message-type 658
match service-type 659
match service-instance 660
mrinfo 661
service-policy-query 663
service-policy 664
show ip igmp filter 665
show ip igmp profile 666
show ip igmp snooping 667
show ip igmp snooping groups 669
show ip igmp snooping mrouter 670
show ip igmp snooping querier 671
show ip pim autorp 673
show ip pim bsr-router 674
show ip pim bsr 675
show ip pim snooping 676
show ip pim tunnel 679
show platform software fed switch ip multicast 681

PART VI Layer 2/3 683

CHAPTER 7 Layer 2/3 Commands 685
channel-group 688
channel-protocol 691
clear l2protocol-tunnel counters 692

clear lacp 693
clear pagp 694
clear spanning-tree counters 695
clear spanning-tree detected-protocols 696
debug etherchannel 697
debug lacp 698
debug pagp 699
debug platform pm 700
debug platform udld 701
debug spanning-tree 702
instance (VLAN) 704
interface port-channel 706
l2protocol-tunnel 708
l2protocol-tunnel cos 711
lacp max-bundle 712
lacp port-priority 713
lacp rate 714
lacp system-priority 715
name (MST) 716
pagp learn-method 717
pagp port-priority 719
port-channel 720
port-channel auto 721
port-channel load-balance 722
port-channel load-balance extended 724
port-channel min-links 725
rep admin vlan 726
rep block port 727
rep lsl-age-timer 729
rep lsl-retries 730
rep preempt delay 731
rep preempt segment 732
rep segment 733
rep stcn 735

revision 736
show dot1q-tunnel 737
show etherchannel 738
show interfaces rep detail 741
show l2protocol-tunnel 742
show lacp 744
show pagp 748
show platform etherchannel 750
show platform pm 751
show rep topology 752
show spanning-tree 754
show spanning-tree mst 760
show udld 763
spanning-tree backbonefast 767
spanning-tree bpdufilter 768
spanning-tree bpduguard 770
spanning-tree bridge assurance 772
spanning-tree cost 773
spanning-tree etherchannel guard misconfig 775
spanning-tree extend system-id 777
spanning-tree guard 778
spanning-tree link-type 779
spanning-tree loopguard default 781
spanning-tree mode 782
spanning-tree mst 783
spanning-tree mst configuration 784
spanning-tree mst forward-time 786
spanning-tree mst hello-time 787
spanning-tree mst max-age 788
spanning-tree mst max-hops 789
spanning-tree mst pre-standard 790
spanning-tree mst priority 792
spanning-tree mst root 793
spanning-tree mst simulate pvst global 794

spanning-tree pathcost method 795
spanning-tree port-priority 796
spanning-tree portfast edge bpdufilter default 798
spanning-tree portfast edge bpduguard default 800
spanning-tree portfast default 801
spanning-tree transmit hold-count 803
spanning-tree uplinkfast 804
spanning-tree vlan 805
switchport 808
switchport access vlan 809
switchport mode 810
switchport nonegotiate 812
switchport voice vlan 813
udld 816
udld port 818
udld reset 820
vlan dot1q tag native 821

PART VII **Network Management** 823

CHAPTER 8 **Network Management Commands** 825
event manager applet 827
ip wccp 830
map platform-type 832
match platform-type 833
monitor capture (interface/control plane) 834
monitor capture buffer 836
monitor capture export 837
monitor capture limit 838
monitor capture start 839
monitor capture stop 840
monitor session destination 841
monitor session filter 845
monitor session source 847

show class-map type control subscriber 849
show ip sla statistics 850
show monitor 852
show monitor capture 854
show parameter-map type subscriber attribute-to-service 856
show platform software fed switch ip wccp 857
show platform software swspan 859
snmp ifmib ifindex persist 861
snmp-server enable traps 862
snmp-server enable traps bridge 865
snmp-server enable traps bulkstat 866
snmp-server enable traps call-home 867
snmp-server enable traps cef 868
snmp-server enable traps cpu 869
snmp-server enable traps envmon 870
snmp-server enable traps errdisable 871
snmp-server enable traps flash 872
snmp-server enable traps isis 873
snmp-server enable traps license 874
snmp-server enable traps mac-notification 875
snmp-server enable traps ospf 876
snmp-server enable traps pim 877
snmp-server enable traps port-security 878
snmp-server enable traps power-ethernet 879
snmp-server enable traps snmp 880
snmp-server enable traps storm-control 881
snmp-server enable traps stpx 882
snmp-server enable traps transceiver 883
snmp-server enable traps vrfmib 884
snmp-server enable traps vstack 885
snmp-server engineID 886
snmp-server group 887
snmp-server host 891
snmp-server user 896

snmp-server view 900
switchport mode access 902
switchport voice vlan 903

CHAPTER 9 **Flexible NetFlow Commands** 905

cache 907
clear flow exporter 909
clear flow monitor 910
collect 912
collect counter 913
collect interface 914
collect timestamp absolute 915
collect transport tcp flags 916
datalink flow monitor 917
debug flow exporter 918
debug flow monitor 919
debug flow record 920
debug sampler 921
description 922
destination 923
dscp 924
export-protocol netflow-v9 925
export-protocol netflow-v5 926
exporter 927
flow exporter 928
flow monitor 929
flow record 930
ip flow monitor 931
ipv6 flow monitor 933
match datalink dot1q priority 935
match datalink dot1q vlan 936
match datalink ethertype 937
match datalink mac 938
match datalink vlan 939

match flow cts 940
match flow direction 941
match interface 942
match ipv4 943
match ipv4 destination address 944
match ipv4 source address 945
match ipv4 ttl 946
match ipv6 947
match ipv6 destination address 948
match ipv6 hop-limit 949
match ipv6 source address 950
match transport 951
match transport icmp ipv4 952
match transport icmp ipv6 953
mode random 1 out-of 954
option 955
record 957
sampler 958
show flow exporter 959
show flow interface 961
show flow monitor 963
show flow record 968
show sampler 969
source 971
template data timeout 973
transport 974
ttl 975

PART VIII QoS 977

CHAPTER 10 QoS Commands 979
auto qos classify 980
auto qos trust 982
auto qos video 989

auto qos voip 999
class 1013
class-map 1015
debug auto qos 1017
match (class-map configuration) 1018
policy-map 1021
priority 1023
queue-buffers ratio 1025
queue-limit 1026
random-detect cos 1028
random-detect cos-based 1029
random-detect dscp 1030
random-detect dscp-based 1032
random-detect precedence 1033
random-detect precedence-based 1035
service-policy (Wired) 1036
set 1038
show auto qos 1044
show class-map 1046
show platform hardware fed switch 1047
show platform software fed switch qos 1050
show platform software fed switch qos qsb 1051
show policy-map 1054
show tech-support qos 1056
trust device 1058

PART IX **Routing** 1061

CHAPTER 11 **IP Routing Commands** 1063

accept-lifetime 1065
address-family ipv6 (OSPF) 1068
area nssa 1069
area virtual-link 1071
authentication (BFD) 1074

bfd 1075
bfd all-interfaces 1077
bfd check-ctrl-plane-failure 1078
bfd echo 1079
bfd slow-timers 1081
bfd template 1083
bfd-template single-hop 1084
default-information originate (OSPF) 1085
distance (OSPF) 1087
eigrp log-neighbor-changes 1090
eigrp log-neighbor-warnings 1092
ip authentication key-chain eigrp 1094
ip authentication mode eigrp 1095
ip bandwidth-percent eigrp 1096
ip cef load-sharing algorithm 1097
ip prefix-list 1098
ip hello-interval eigrp 1101
ip hold-time eigrp 1102
ip load-sharing 1103
ip ospf database-filter all out 1104
ip ospf name-lookup 1105
ip split-horizon eigrp 1106
ip summary-address eigrp 1107
ip route static bfd 1109
ipv6 route static bfd 1111
metric weights (EIGRP) 1112
neighbor description 1114
network (EIGRP) 1115
nsf (EIGRP) 1117
offset-list (EIGRP) 1119
redistribute (IP) 1121
redistribute (IPv6) 1129
redistribute maximum-prefix (OSPF) 1132
route-map 1134

router-id 1137
router eigrp 1138
router ospfv3 1139
send-lifetime 1140
show ip eigrp interfaces 1143
show ip eigrp neighbors 1146
show ip eigrp topology 1149
show ip eigrp traffic 1154
show ip ospf 1156
show ip ospf border-routers 1164
show ip ospf database 1165
show ip ospf interface 1174
show ip ospf neighbor 1177
show ip ospf virtual-links 1183
summary-address (OSPF) 1184
timers throttle spf 1186

PART X Security 1189

CHAPTER 12 Security 1191
aaa accounting 1194
aaa accounting dot1x 1197
aaa accounting identity 1199
aaa authentication dot1x 1201
aaa new-model 1202
authentication host-mode 1204
authentication logging verbose 1206
authentication mac-move permit 1207
authentication priority 1209
authentication violation 1211
cisp enable 1213
cisp enable 1214
clear device-tracking database 1215
clear errdisable interface vlan 1219

clear mac address-table 1220
confidentiality-offset 1222
debug aaa dead-criteria transaction 1223
delay-protection 1225
deny (MAC access-list configuration) 1226
device-role (IPv6 snooping) 1229
device-role (IPv6 nd inspection) 1230
device-tracking (interface config) 1231
device-tracking (VLAN config) 1234
device-tracking binding 1237
device-tracking logging 1257
device-tracking policy 1261
device-tracking tracking 1274
device-tracking upgrade-cli 1278
dot1x critical (global configuration) 1281
dot1x logging verbose 1282
dot1x pae 1283
dot1x supplicant controlled transient 1284
dot1x supplicant force-multicast 1285
dot1x test eapol-capable 1286
dot1x test timeout 1287
dot1x timeout 1288
dtls 1290
enable password 1292
enable secret 1294
epm access-control open 1297
include-icv-indicator 1298
ip access-list 1299
ip access-list role-based 1302
ip admission 1303
ip admission name 1304
ip dhcp snooping database 1306
ip dhcp snooping information option format remote-id 1308
ip dhcp snooping verify no-relay-agent-address 1309

ip http access-class 1310
ip radius source-interface 1312
ip source binding 1314
ip ssh source-interface 1315
ip verify source 1316
ipv6 access-list 1317
ipv6 snooping policy 1319
key chain macsec 1320
key config-key password-encrypt 1321
key-server 1323
limit address-count 1324
mab logging verbose 1325
mab request format attribute 32 1326
macsec-cipher-suite 1328
macsec network-link 1329
match (access-map configuration) 1330
mka pre-shared-key 1332
mka suppress syslogs sak-rekey 1333
password encryption aes 1334
permit (MAC access-list configuration) 1336
protocol (IPv6 snooping) 1339
radius server 1340
radius-server dead-criteria 1342
radius-server deadtime 1344
radius-server directed-request 1346
radius-server domain-stripping 1348
sak-rekey 1352
security level (IPv6 snooping) 1353
send-secure-announcements 1354
server-private (RADIUS) 1355
server-private (TACACS+) 1357
show aaa clients 1359
show aaa command handler 1360
show aaa dead-criteria 1361

show aaa local 1363
show aaa servers 1365
show aaa sessions 1366
show authentication brief 1367
show authentication sessions 1370
show cisp 1373
show device-tracking capture-policy 1375
show device-tracking counters 1377
show device-tracking database 1379
show device-tracking events 1384
show device-tracking features 1386
show device-tracking messages 1387
show device-tracking policies 1388
show device-tracking policy 1389
show dot1x 1390
show eap pac peer 1392
show ip access-lists 1393
show ip dhcp snooping statistics 1396
show radius server-group 1399
show tech-support acl 1401
show tech-support identity 1405
show vlan access-map 1414
show vlan filter 1415
show vlan group 1416
ssci-based-on-sci 1417
switchport port-security aging 1418
switchport port-security mac-address 1420
switchport port-security maximum 1423
switchport port-security violation 1425
tacacs server 1427
tracking (IPv6 snooping) 1428
trusted-port 1430
use-updated-eth-header 1431
username 1432

vlan access-map 1437
vlan dot1Q tag native 1439
vlan filter 1440
vlan group 1441

PART XI Stack Manager and High Availability 1443

CHAPTER 13 Stack Manager and High Availability Commands 1445

main-cpu 1446
mode sso 1447
policy config-sync prc reload 1448
redundancy 1449
redundancy config-sync mismatched-commands 1450
redundancy force-switchover 1452
redundancy reload 1453
reload 1454
show redundancy 1455
show redundancy config-sync 1459
show switch 1461
show switch stack-mode 1464
stack-mac persistent timer 1465
stack-mac update force 1467
standby console enable 1468
switch clear stack-mode 1469
switch switch-number role 1470
switch stack port 1471
switch priority 1472
switch provision 1473
switch renumber 1475
switch renumber 1476

PART XII System Management 1477

CHAPTER 14 System Management Commands 1479

arp 1481
boot 1482
boot system 1483
cat 1484
copy 1485
copy startup-config tftp: 1486
copy tftp: startup-config 1487
debug voice diagnostics mac-address 1488
debug platform condition feature multicast controlplane 1489
debug platform condition mac 1491
debug platform rep 1492
debug ilpower powerman 1493
delete 1496
dir 1497
exit 1499
factory-reset 1500
flash_init 1502
help 1503
install 1504
l2 traceroute 1508
license boot level 1509
license smart deregister 1511
license smart register idtoken 1512
license smart renew 1513
location 1514
location plm calibrating 1517
mgmt_init 1518
mkdir 1519
more 1520
no debug all 1521
rename 1522
request consent-token accept-response shell-access 1523
request consent-token generate-challenge shell-access 1524
request consent-token terminate-auth 1525

request platform software console attach switch 1526
reset 1528
rmdir 1529
sdm prefer 1530
service private-config-encryption 1531
set 1532
show avc client 1535
show debug 1536
show env xps 1537
show flow monitor 1541
show install 1546
show license all 1548
show license status 1550
show license summary 1552
show license udi 1553
show license usage 1554
show location 1555
show logging onboard switch uptime 1557
show mac address-table 1560
show mac address-table move update 1565
show parser encrypt file status 1566
show platform integrity 1567
show platform software audit 1568
show platform software fed switch punt cause 1572
show platform software fed switch punt cpuq 1574
show platform sudi certificate 1577
show running-config 1579
show sdm prefer 1585
show tech-support license 1587
show tech-support platform 1589
show tech-support platform evpn_vxlan 1593
show tech-support platform fabric 1595
show tech-support platform igmp_snooping 1599
show tech-support platform layer3 1602

show tech-support platform mld_snooping 1610
show tech-support port 1617
show version 1620
system env temperature threshold yellow 1627
traceroute mac 1628
traceroute mac ip 1631
type 1633
unset 1634
version 1636

CHAPTER 15 Tracing 1637
Information About Tracing 1638
Tracing Overview 1638
Location of Tracelogs 1638
Tracelog Naming Convention 1638
Rotation and Throttling Policy 1639
Tracing Levels 1639
set platform software trace 1640
show platform software trace filter-binary 1644
show platform software trace message 1645
show platform software trace level 1648
request platform software trace archive 1651
request platform software trace rotate all 1652
request platform software trace filter-binary 1653

PART XIII VLAN 1655

CHAPTER 16 VLAN Commands 1657
clear vtp counters 1658
debug sw-vlan 1659
debug sw-vlan ifs 1661
debug sw-vlan notification 1662
debug sw-vlan vtp 1663
private-vlan 1665

private-vlan mapping 1667
show interfaces private-vlan mapping 1669
show vlan 1670
show vtp 1674
switchport mode private-vlan 1679
switchport priority extend 1681
switchport trunk 1682
vlan 1685
vlan dot1q tag native 1691
vtp (global configuration) 1692
vtp (interface configuration) 1697
vtp primary 1698

Using the Command-Line Interface

This chapter contains the following topics:

- Using the Command-Line Interface, on page 2

Using the Command-Line Interface

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

Understanding Command Modes

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

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

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

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

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

Table 1: Command Mode Summary

Mode	Access Method	Prompt	Exit Method	About This Mode
User EXEC	Begin a session with your switch.	`Switch>`	Enter **logout** or **quit**.	Use this mode to • Change terminal settings. • Perform basic tests. • Display system information.
Privileged EXEC	While in user EXEC mode, enter the **enable** command.	`#`	Enter **disable** to exit.	Use this mode to verify commands that you have entered. Use a password to protect access to this mode.
Global configuration	While in privileged EXEC mode, enter the **configure** command.	`(config)#`	To exit to privileged EXEC mode, enter **exit** or **end**, or press **Ctrl-Z**.	Use this mode to configure parameters that apply to the entire switch.

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

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

Understanding the Help System

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

Table 2: Help Summary

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

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

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

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

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

Understanding Abbreviated Commands

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

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

```
# show conf
```

Understanding no and default Forms of Commands

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

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

Understanding CLI Error Messages

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

Table 3: Common CLI Error Messages

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

Using Configuration Logging

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

Note Only CLI or HTTP changes are logged.

Using Command History

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

Changing the Command History Buffer Size

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

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

```
# 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:

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

The range is from 0 to 256.

Recalling Commands

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

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

Table 4: Recalling Commands

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

Disabling the Command History Feature

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

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

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

Using Editing Features

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

Enabling and Disabling Editing Features

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

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

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

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

```
# terminal editing
```

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

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

Editing Commands through Keystrokes

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

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

Table 5: Editing Commands through Keystrokes

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

Capability	Keystroke	Purpose
Recall commands from the buffer and paste them in the command line. The switch provides a buffer with the last ten items that you deleted.	Press **Ctrl-Y.**	Recalls the most recent entry in the buffer.
	Press **Esc Y**.	Recalls the next buffer entry. The buffer contains only the last 10 items that you have deleted or cut. If you press **Esc Y** more than ten times, you cycle to the first buffer entry.
Delete entries if you make a mistake or change your mind.	Press the **Delete** or **Backspace** key.	Erases the character to the left of the cursor.
	Press **Ctrl-D**.	Deletes the character at the cursor.
	Press **Ctrl-K**.	Deletes all characters from the cursor to the end of the command line.
	Press **Ctrl-U** or **Ctrl-X**.	Deletes all characters from the cursor to the beginning of the command line.
	Press **Ctrl-W**.	Deletes the word to the left of the cursor.
	Press **Esc D**.	Deletes from the cursor to the end of the word.
Capitalize or lowercase words or capitalize a set of letters.	Press **Esc C**.	Capitalizes at the cursor.
	Press **Esc L**.	Changes the word at the cursor to lowercase.
	Press **Esc U**.	Capitalizes letters from the cursor to the end of the word.
Designate a particular keystroke as an executable command, perhaps as a shortcut.	Press **Ctrl-V** or **Esc Q**.	

Capability	Keystroke	Purpose
Scroll down a line or screen on displays that are longer than the terminal screen can display. **Note** The More prompt is used for any output that has more lines than can be displayed on the terminal screen, including **show** command output. You can use the **Return** and **Space** bar keystrokes whenever you see the More prompt.	Press the **Return** key.	Scrolls down one line.
	Press the **Space** bar.	Scrolls down one screen.
Redisplay the current command line if the switch suddenly sends a message to your screen.	Press **Ctrl-L** or **Ctrl-R**.	Redisplays the current command line.

Editing Command Lines that Wrap

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

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

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

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

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

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

```
(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:

```
# 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 switch member interfaces through the active switch. You cannot manage switch 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 switch 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 switch member port, you must include the switch member number in the CLI command interface notation.

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

Accessing the CLI through a Console Connection or through Telnet

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

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

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

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

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

  The switch supports up to five simultaneous secure SSH sessions.

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

PART I

Cisco SD-Access

- Cisco SD-Access Commands, on page 15

Cisco SD-Access Commands

- broadcast-underlay, on page 17
- database-mapping, on page 18
- dynamic-eid, on page 20
- eid-record-provider, on page 21
- eid-record-subscriber, on page 22
- eid-table, on page 23
- encapsulation, on page 25
- etr, on page 26
- etr map-server, on page 27
- extranet, on page 28
- instance-id, on page 29
- ip pim lisp core-group-range, on page 30
- ip pim lisp transport multicast, on page 31
- ip pim rp-address, on page 32
- ip pim sparse mode, on page 33
- ipv4 multicast multitopology, on page 34
- ip pim ssm, on page 35
- itr, on page 36
- itr map-resolver, on page 37
- locator default-set, on page 38
- locator-set, on page 39
- map-cache , on page 40
- map-cache extranet, on page 41
- prefix-list, on page 42
- route-import database, on page 43
- service, on page 45
- show lisp instance-id ipv4 database, on page 46
- show lisp instance-id ipv6 database, on page 48
- show lisp instance-id ipv4 map-cache, on page 49
- show lisp instance-id ipv6 map-cache, on page 55
- show lisp instance-id ipv4 server, on page 57
- show lisp instance-id ipv6 server, on page 59
- show lisp instance-id ipv4 statistics, on page 60

- show lisp instance-id ipv6 statistics, on page 61
- show lisp prefix-list, on page 62
- show lisp session, on page 63
- use-petr, on page 64

broadcast-underlay

To configure the underlay in a LISP network to use a mutlicast group to send encapsulated broadcast packets and link local multicast packets, use the **broadcast-underlay** command in the service submode.

[**no**] **broadcast-underlay** *multicast-ip*

Syntax Description

multicast-ip	The IP address of the multicast group used to send the encapsulated broadcast packets

Command Default

None.

Command Modes

LISP Service Ethernet (router-lisp-inst-serv-eth)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1c	This command was introduced.

Usage Guidelines

Use this command to enable the broadcast functionality on the fabric edge node in a LISP network. Ensure that this command is used in the router-lisp-service-ethernet mode or router-lisp-instance-service-ethernet mode.

Use the **no** form of the command to remove the broadcast functionality.

The following example shows how to configure broadcast on a fabric edge node:

```
device(config)#router lisp
device(config-router-lisp)#instance-id 3
device(config-router-lisp-inst)#service ethernet
device(config-router-lisp-inst-serv-eth)#eid-table vlan 250
device(config-router-lisp-inst-serv-eth)#broadcast-underlay 225.1.1.1
device(config-router-lisp-inst-serv-eth)#database-mapping mac locator-set rloc2
device(config-router-lisp-inst-serv-eth)#exit-service-ethernet
```

database-mapping

To configure an IPv4 or IPv6 endpoint identifier-to-routing locator (EID-to-RLOC) mapping relationship and an associated traffic policy for Locator/ID Separation Protocol (LISP), use the **database-mapping** command in the LISP EID-table configuration mode. To remove the configured database mapping, use the **no** form of the command.

[**no**] **database-mapping** {*eid-prefix / prefix-length* [**locator-set** *RLOC-name* **proxy**] | **ip-interface** *interface-name* | **ipv6-interface** *interface-name* | **ipv4-interface** *interface-name* | **auto-discover-rlocs**] | **limit**}

Syntax Description

eid-prefix / prefix-length	Specifies the IPv4 or IPv6 endpoint identifier prefix and length that is advertised by the router.
locator-set *RLOC-name*	Specifies the routing locator (RLOC) associated with the value specified for the eid-prefix.
proxy	Enables configuration of static proxy database mapping.
ipv4 interface *interface-name*	Specifies the IPv4 address and name of the interface to be used as the RLOC for the EID prefix.
ipv6 interface *interface-name*	Specifies the IPv6 address and name of the interface to be used as the RLOC for the EID prefix.
auto-discover-rlocs	Configures the Egress Tunnel Router (ETR) to discover the locators of all routers configured to function as both an ETR and an Ingress Tunnel Router (ITR)—such routers are referred to as xTRs—in the ETR LISP site when the site uses multiple xTRs and each xTR is configured to use DHCP-learned locators or configured with only its own locators.
limit	Specifies the maximum size of local EID prefixes database.

Command Default

No LISP database entries are defined.

Command Modes

LISP Instance Service (router-lisp-instance-service)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1c	This command was introduced.

Usage Guidelines

In the LISP-instance-service configuration mode, the **database-mapping** command configures LISP database parameters a specified IPv4 or IPv6 EID-prefix block. The *locator* is the IPv4 or IPv6 address of any interface used as the RLOC address for the eid-prefix assigned to the site but can also be the loopback address of the interface.

When a LISP site has multiple locators associated with the same EID-prefix block, multiple **database-mapping** commands are used to configure all of the locators for a given EID-prefix block.

In a multi-site scenario, the LISP border node advertises the site EID that it's attached to towards the transit map-server to attract site traffic. To do this, it has to obtain the route from the internal border and proxy register

with the transit site map-server accordingly. The **database-mapping** command has the **proxy** keyword to enable configuration of a static proxy database mapping.

The following example shows how to map the eid-prefix with the locator-set, RLOC, in the EID configuration mode, on an external border:

Note Ensure that the locator-set RLOC is already configured.

```
device(config)# router lisp
device(config-router-lisp)# instance-id 3
device(config-router-lisp-inst)# service ipv4
device(config-router-lisp-inst-serv-ipv4)#eid-table vrf red
device(config-router-lisp-inst-serv-ipv4-eid-table)# database-mapping 172.168.0.0/16
locator-set RLOC proxy
device(config-router-lisp-inst-serv-ipv4-eid-table)# database-mapping 173.168.0.0/16
locator-set RLOC proxy
device(config-router-lisp-inst-serv-ipv4-eid-table)# map-cache 0.0.0.0/0 map-request
device(config-router-lisp-inst-serv-ipv4-eid-table)#exit
device(config-router-lisp-inst-serv-ipv4)#
```

Related Commands

Command D	Description
eid-table vrf *vrf-name*	Associates the instance-service instantiation with a virtual routing and forwarding (VRF) table or default table through which the endpoint identifier address space is reachable.

dynamic-eid

To create a dynamic End Point Identifier (EID) policy and enter the dynamic-eid configuration mode on an xTR, use the **dynamic-eid** command.

dynamic-eid *eid-name*

Syntax Description

eid-name	If *eid-name* exists, it enters *eid-name* configuration mode. Else, a new dynamic-eid policy with name *eid-name* is created and it enters the dynamic-eid configuration mode.

Command Default

No LISP dynamic-eid policies are configured.

Command Modes

LISP EID-table (router-lisp-eid-table)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1c	This command was introduced.

Usage Guidelines

To configure LISP mobility, create a dynamic-EID roaming policy that can be referenced by the **lisp mobility** interface command. When the **dynamic-eid** command is entered, the referenced LISP dynamic-EID policy is created and you enter the dynamic-EID configuration mode. In this mode, all attributes associated with the referenced LISP dynamic-EID policy can be entered. When a dynamic-EID policy is configured, you must specify the dynamic-EID-to-RLOC mapping relationship and its associated traffic policy.

Related Commands

Command D	Description
lisp mobility	Configures an interface on an ITR to participate in LISP mobility (dynamic-EID roaming).

eid-record-provider

To define the extranet policy table for the provider instance use the **eid-record-provider** command in the lisp-extranet mode.

[**no**] **eid-record-provider instance-id** *instance id* {*ipv4 address prefix* | *ipv6 address prefix*} **bidirectional**

Syntax Description

instance-id *instance id*	The instance-id of the LISP instance for which the extranet provider policy applies.
ipv4 address prefix	Defines the IPv4 EID prefixes to be leaked, specified in a.b.c.d/nn form.
ipv6 address prefix	Defines the IPv6 EID prefixes to be leaked, prefix specified in X:X:X:X::X/<0-128> form.
bidirectional	Specifies that the extranet communication between the provider and subscriber EID prefixes are bidirectional.

Command Default

None.

Command Modes

router-lisp-extranet

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1c	This command was introduced.

Usage Guidelines

Use the **no** form of the command to negate the eid-record-provider configuration.

```
device(config)#router lisp
device(config-router-lisp)#extranet ext1
device(config-router-lisp-extranet)#eid-record-provider instance-id 5000 10.0.0.0/8
bidirectional
device(config-router-lisp-extranet)#eid-record-subscriber instance-id 1000 3.0.0.0/24
bidirectional
```

eid-record-subscriber

To define the extranet policy table for the subscriber instance use the **eid-record-subscriber** command in the lisp-extranet mode.

[**no**] **eid-record-subscriber instance-id** *instance id* {*ipv4 address prefix* | *ipv6 address prefix*} **bidirectional**

Syntax Description

instance-id *instance id*	The instance-id of the LISP instance for which the extranet provider policy applies.
ipv4 address prefix	Defines the IPv4 EID prefixes to be leaked, specified in a.b.c.d/nn form.
ipv6 address prefix	Defines the IPv6 EID prefixes to be leaked, prefix specified in X:X:X:X::X/<0-128> form.
bidirectional	Specifies that the extranet communication between the provider and subscriber EID prefixes are bidirectional.

Command Default

None.

Command Modes

LISP Extranet (router-lisp-extranet)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1c	This command was introduced.

Usage Guidelines

Use the **no** form of the command to negate the eid-record-subscriber configuration.

```
device(config)#router lisp
device(config-router-lisp)#extranet ext1
device(config-router-lisp-extranet)#eid-record-provider instance-id 5000 10.0.0.0/8
bidirectional
device(config-router-lisp-extranet)#eid-record-subscriber instance-id 1000 3.0.0.0/24
bidirectional
device(config-router-lisp-extranet)#eid-record-subscriber instance-id 2000 20.20.0.0/8
bidirectional
```

eid-table

The **eid-table** command associates the instance-service instantiation with a virtual routing and forwarding (VRF) table or default table through which the endpoint identifier address space is reachable.

[**no**] **eid-table** {*vrf-name* | **default** | **vrf** *vrf-name*}

Syntax Description

default	Selects the default (global) routing table for association with the configured instance-service.
vrf *vrf-name*	Selects the named VRF table for association with the configured instance.

Command Default

Default VRF is associated with instance-id 0.

Command Modes

router-lisp-instance-service

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1c	This command was introduced.

Usage Guidelines

This command is used only in the instance-service mode.

For Layer 3 (service ipv4 / service ipv6), a VRF table is associated with the instance-service. For Layer 2 (service ethernet), a VLAN is associated with the instance-service.

Note For Layer 2, ensure that you have defined a VLAN before configuring the eid-table.

For Layer 3, ensure that you have defined a VRF table before you configure the eid-table.

In the following example, an XTR is configured to segment traffic using VRF named vrf-table. The EID prefix associated with vrf-table is connected to instance ID 3.

```
device(config)#vrf definition vrf-table
device(config-vrf)#address-family ipv4
device(config-vrf-af)#exit
device(config-vrf)#exit
device(config)#router lisp
device(config-router-lisp)#instance-id 3
device(config-router-lisp-inst)#service ipv4
device(config-router-lisp-inst-serv-ipv4)#eid-table vrf vrf-table
```

In the following example, the EID prefix associated with a VLAN, named Vlan10, is connected to instance ID 101.

```
device(config)#interface Vlan10
device(config-if)#mac-address ba25.cdf4.ad38
device(config-if)#ip address 10.1.1.1 255.255.255.0
device(config-if)#end
device(config)#router lisp
device(config-router-lisp)#instance-id 101
device(config-router-lisp-inst)#service ethernet
```

```
device(config-router-lisp-inst-serv-ethernet)#eid-table Vlan10
device(config-router-lisp-inst-serv-ethernet)#database-mapping mac locator-set set
device(config-router-lisp-inst-serv-ethernet)#exit-service-etherne
device(config-router-lisp-inst)#exit-instance-id
```

encapsulation

To configure the type of encapsulation of the data packets in the LISP network, use the **encapsulation** command in the service mode.

[**no**] **encapsulation** {**vxlan | lisp**}

Syntax Description

encapsulation vxlan	Specifies VXLAN-based encapsulation.
encapsulation lisp	Specifies LISP-based encapsulation

Command Default

None.

Command Modes

LISP Service IPv4 (router-lisp-serv-ipv4)

LISP Service IPv6 (router-lisp-serv-ipv6)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1c	This command was introduced.

Usage Guidelines

Use the **encapsulation vxlan** command in the service ethernet mode to encapuslate Layer 2 packets. Use the **encapsulation lisp** command in the service ipv4 or service ipv6 mode to encapsulate the Layer 3 packets.

Use the **no** form of the command to remove encapsulation on the packets.

The following example shows how to configure an xTR for data encapsulation

```
device(config)#router lisp
device(config-router-lisp)#service ipv4
device(config-router-lisp-serv-ipv4)#encapuslation vxlan
device(config-router-lisp-serv-ipv4)#map-cache-limit 200
device(config-router-lisp-serv-ipv4)#exit-service-ipv4
```

etr

To configure a device as an Egress Tunnel Router (ETR) use the **etr** command in the instance-service mode or service submode.

[**no**] **etr**

Command Default

The device is not configured as ETR by default.

Command Modes

router-lisp-instance-service

router-lisp-service

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1c	This command was introduced.

Usage Guidelines

Use this command to enable a device to perform the ETR functionality.

Use the **no** form of the command to remove the ETR functionality.

A router configured as an ETR is also typically configured with database-mapping commands so that the ETR knows what endpoint identifier (EID)-prefix blocks and corresponding locators are used for the LISP site. In addition, the ETR should be configured to register with a map server with the **etr map-server** command, or to use static LISP EID-to-routing locator (EID-to-RLOC) mappings with the **map-cache** command to participate in LISP networking.

The following example shows how to configure a device as an ETR.

```
device(config)#router lisp
device(config-router-lisp)#instance-id 3
device(config-router-lisp-inst)#service ipv4
device(config-router-lisp-inst-serv-ipv4)#etr
```

etr map-server

To configure a map server to be used by the Egress Tunnel Router (ETR) when configuring the EIDs, use the **etr map-server** command in the instance mode or instance-service mode. To remove the configured locator address of the map-server, use the **no** form of this command.

etr map-server *map-server-address* {**key** [**0** | **6** | **7**] *authentication-key* | **proxy-reply** }

Syntax Description

map-server-address	The locator address of the map server.
key	Specifies the key type.
0	Indicates that password is entered as clear text.
6	Indicates that password is in the AES encrypted form.
7	Indicates that passowrd is a weak encrypted one.
authentication-key	The password used for computing the SHA-1 HMAC hash that is included in the header of the map-register message.
proxy-reply	Specifies that the map server answer the map-requests on behalf the ETR.

Command Default

None.

Command Modes

LISP Instance Service (router-lisp-inst-serv)

LISP Service (router-lisp-serv)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1c	This command was introduced.

Usage Guidelines

Use the **etr map-server** command to configure the locator of the map server to which the ETR will register for its EIDs. The authentication key argument in the command syntax is a password that is used for a SHA-1 HMAC hash (included in the header of the map-register message). The password used for the SHA-1 HMAC may be entered in unencrypted (cleartext) form or encrypted form. To enter an unencrypted password, specify 0. To enter an AES encrypted password, specify 6.

Use the **no** form of the command to remove the map server functionality.

The following example shows how to configure a map server located at 2.1.1.6 to act as a proxy in order to answer the map-requests on the ETR .

```
device(config)#router lisp
device(config-router-lisp)#instance-id 3
device(config-router-lisp-inst)#service ipv4
device(config-router-lisp-inst-serv-ipv4)#etr map-server 2.1.1.6 key foo
device(config-router-lisp-inst-serv-ipv4)#etr map-server 2.1.1.6 proxy-reply
```

extranet

To enable the inter-VRF communication in a LISP network, use the **extranet** command in the LISP configuration mode on the MSMR.

extranet *name-extranet*

Syntax Description

name-extranet	Specifies the name of the extranet created.

Command Default

None.

Command Modes

LISP (router-lisp)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1c	This command was introduced.

```
device(config)#router lisp
device(config-router-lisp)#extranet ext1
device(config-router-lisp-extranet)#
```

instance-id

To creae a LISP EID instance under the router-lisp configuration mode and enter the instance-id submode, use the **instance-id** command.

instance-id *iid*

Command Default

None.

Command Modes

LISP (router-lisp)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1c	This command was introduced.

Usage Guidelines

Use the instance-id command to create a LISP eid instance to group multiple services.

Configuration under this instance-id will apply to all services underneath it.

```
device(config)#router lisp
device(config-router-lisp)#instance-id 3
device(config-router-lisp-inst)#
```

ip pim lisp core-group-range

To configure the core range of address of a Protocol Independent Multicast (PIM) Source Specific Multicast (SSM) on a LISP sub-interface, use the **ip pim lisp core-group-range** command in interface configuration mode. To remove SSM address range, use the **no** form of this command

[**no**] **ip pim lisp core-group-range** *start-SSM-address range-size*

Syntax Description

start-SSM-address	Specifies the start of the SSM IP address range.
number-of-groups	Specifies the size of group range.

Command Default

By default the group range 232.100.100.1 to 232.100.100.255 is assigned if a core range of addresses is not configured.

Command Modes

LISP Interface Configuration (config-if)

Command History

Release	Modification
Cisco IOS XE 16.9.1	This command was introduced.

Usage Guidelines

Native multicast transport supports only PIM SSM in the underlay or the core. Multicast transport uses a grouping mechanism to map the end-point identifiers (EID) entries to the RLOC space SSM group entries. By default, the group range 232.100.100.1 to 232.100.100.255 is used as the SSM range of addresses on a LISP interface to transport multicast traffic. Use the **ip pim lisp core-group-range** command to manually change this SSM core group range of IP addresses on the LISP interfaces.

The following example defines a group of 1000 IP addresses starting from 232.0.0.1 as the SSM range of addresses on the core for multicast traffic.

```
Device(config)#interface LISP0.201
Device(config-if)#ip pim lisp core-group-range 232.0.0.1 1000
```

ip pim lisp transport multicast

To enable multicast as the transport mechanism on LISP interface and sub-interface, use the **ip pim lisp transport multicast** command in the LISP Interface Configuration mode. To disable multicast as the transport mechanism on the LISP interface, use the **no** form of this command

[**no**] **ip pim lisp transport multicast**

Syntax Description

This command has no keywords or arguments.

Command Default

If this command is not configured, head-end replication is used for multicast.

Command Modes

LISP Interface Configuration (config-if)

Command History

Release	Modification
Cisco IOS XE 16.9.1	This command was introduced.

Example

The following example configures multicast as the transport mechanism on a LISP Interface:

```
Device(config)#interface LISP0
 Device(config-if)#ip pim lisp transport multicast
```

Related Commands

Command	Description
ip multicast routing	Enables ip multicast routing or multicast distributed switching.

ip pim rp-address

To configure the address of a Protocol Independent Multicast (PIM) rendezvous point (RP) for a particular group, use the **ip pim rp-address** command in global configuration mode. To remove an RP address, use the **no** form of this command

[**no**] **ip pim** [**vrf***vrf-name*] **rp-address** *rp-address* [*access-list*]

Syntax Description

vrf	Optional) Specifies the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
rp-address	IP address of a router to be a PIM RP. This is a unicast IP address in four-part dotted-decimal notation.
access-list	(Optional) Number or name of an access list that defines the multicast groups for which the RP should be used.

Command Default

None.

Command Modes

Global Configuration (config)

Command History

Release	Modification
Cisco IOS XE 16.8.1s	This command was introduced.

Usage Guidelines

Use the **ip pim rp-address** command to statically define the RP address for multicast groups that are to operate in sparse mode or bidirectional mode.

You can configure the Cisco IOS software to use a single RP for more than one group. The conditions specified by the access list determine for which groups the RP can be used. 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.

The following example sets the PIM RP address to 185.1.1.1 for all multicast groups:

```
Device(config)#ip pim rp-address 185.1.1.1
```

ip pim sparse mode

To enable sparse mode of operation of Protocol Independent Multicast (PIM) on an interface, use the **ip pim sparse-mode** command in the Interface Configuration mode. To disable the sparse mode of operation use the **no** form of this command

[**no**] **ip pim sparse mode** {

Syntax Description

This command has no keywords or arguments.

Command Default

None.

Command Modes

Interface Configuration (config-if)

Command History

Release	Modification
Cisco IOS XE 16.8.1s	This command was introduced.

Usage Guidelines

The NetFlow **collect** commands are used to configure nonkey fields for the flow monitor record and to enable capturing the values in the fields for the flow created with the record. The values in nonkey fields are added to flows to provide additional information about the traffic in the flows. A change in the value of a nonkey field does not create a new flow.

The following example configures pim sparse mode of operation:

```
Device(config)#interface Loopback0
Device(config-if)#ip address 170.1.1.1 255.255.255.0
Device(config-if)#ip pim sparse-mode
```

Related Commands

Command	Description
ip multicast routing	Enables ip multicast routing or multicast distributed switching..

ipv4 multicast multitopology

To enable Multicast-Specific RPF topology support for IP Multicast routing, use the **ipv4 multicast multitopology** command in the VRF configuration mode. To disable the Multicast-Specific RPF Topology support, use the **no** form of this command.

[**no**] **ipv4 multicast multitopology**

Syntax Description

This command has no arguments or keywords.

Command Default None.

Command Modes VRF Configuration (config-vrf)

Command History

Release	Modification
Cisco IOS XE 16.8.1s	This command was introduced.
Cisco IOS XE Fuji 16.8.1a	

The following example shows how to configure Multicast-Specific RPF Topology:

```
Device(config)#vrf definition VRF1
Device(config-vrf)#ipv4 multicast multitopology
```

ip pim ssm

To define the Source Specific Multicast (SSM) range of IP multicast addresses, use the **ip pim ssm** command in global configuration mode. To disable the SSM range, use the **no** form of this command.

[**no**] **ip pim** [**vrf***vrf-name*] **ssm** {**default** | **range** *access-list*}

Syntax Description

vrf	Optional) Specifies the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
range *access-list*	Specifies the standard IP access list number or name defining the SSM range.
default2	Defines the SSM range access list to 232/8.

Command Default

None.

Command Modes

Global Configuration (config)

Command History

Release	Modification
Cisco IOS XE 16.8.1s	This command was introduced.

Usage Guidelines

When an SSM range of IP multicast addresses is defined by the **ip pim ssm** command, no Multicast Source Discovery Protocol (MSDP) Source-Active (SA) messages will be accepted or originated in the SSM range.

The following example sets the SSM range of IP multicast address to default

```
Device(config)#ip pim ssm default
```

Related Commands

Command	Description
ip multicast routing	Enables ip multicast routing or multicast distributed switching..

itr

To configure a device as an Ingress Tunnel Router (ITR) use the **itr** command in the service submode or instance-service mode.

[**no**] **itr**

Command Default

The device is not configured as ITR by default.

Command Modes

LISP Instance Service (router-lisp-instance-service)

LISP Service (router-lisp-service)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1c	This command was introduced.

Usage Guidelines

Use this command to enable a device to perform the ITR functionality.

Use the **no** form of the command to remove theITR functionality.

A device configured as an ITR helps find the EID-to-RLOC mapping for all traffic destined to LISP-capable sites.

The following example shows how to configure a device as an ITR.

```
device(config)#router lisp
device(config-router-lisp)#instance-id 3
device(config-router-lisp-inst)#service ipv4
device(config-router-lisp-inst-serv-ipv4)#itr
```

itr map-resolver

To configure a device as a map resolver to be used by an Ingress Tunnel Router (ITR) when sending map-requests, use the **itr map-resolver** command in the service submode or instance-service mode.

[**no**] **itr** [**map-resolver** *map-address*] **prefix-list** *prefix-list-name*

Syntax Description

map-resolver *map-address*	Configures map-resolver address for sending map requests, on the ITR.
prefix-list *prefix-list-name*	Specifies the prefix list to be used.

Command Default

None.

Command Modes

router-lisp-instance-service

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1c	This command was introduced.

Usage Guidelines

Use this command to enable a device to perform the ITR map-resolver functionality.

Use the **no** form of the command to remove the map-resolver functionality.

A device configured as a Map Resolver accepts encapsulated Map-Request messages from ITRs, decapsulates those messages, and then forwards the messages to the Map Server responsible for the egress tunnel routers (ETRs) that are authoritative for the requested EIDs. In a multi-site environment, the site border relies on Map Resolver prefix-list to determine whether to query the transit site MSMR or site MSMR.

The following example shows how to configure an ITR to use the map-resolver located at 2.1.1.6 when sending map request messages.

```
device(config)#router lisp
device(config-router-lisp)#prefix-list wired
device(config-router-lisp-prefix-list)#2001:193:168:1::/64
device(config-router-lisp-prefix-list)#192.168.0.0/16
device(config-router-lisp-prefix-list)#exit-prefix-list


device(config-router-lisp)#service ipv4
device(config-router-lisp-serv-ipv4)#encapsulation vxlan
device(config-router-lisp-serv-ipv4)#itr map-resolver 2.1.1.6 prefix-list wired
device(config-router-lisp-serv-ipv4)#
```

locator default-set

To mark a locator-set as default, use the **locator default-set** command at the router-lisp level.

[**no**] **locator default-set** *rloc-set-name*

Syntax Description

rloc-set-name	The name of locator-set that is set as default.

Command Default

None

Command Modes

LISP (router-lisp)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1c	This command was introduced.

Usage Guidelines

The locator-set configured as default with the **locator default-set** command applies to all services and instances.

locator-set

To specify a locator-set and enter the locator-set configuration mode, use the **locator-set** command at the router-lisp level.

[**no**] **locator-set** *loc-set-name*

Syntax Description

loc-set-name	The name of locator-set.

Command Default

Name

Command Modes

LISP (router-lisp)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1c	This command was introduced.

Usage Guidelines

You must first define the locator-set before referring to it.

map-cache

To configure a static endpoint identifier (EID) to routing locator (RLOC) (EID-to-RLOC) mapping relationship, use the **map-cache** command in the instance-service ipv4 or instance-service ipv6 mode.

[**no**] **map-cache** *destination-eid-prefix/prefix-len* { *ipv4-address* { **priority** *priority* **weight** *weight* } | *ipv6-address* | **map-request** | **native-forward** }

Syntax Description

destination-eid-prefix/prefix-len	Destination IPv4 or IPv6 EID-prefix/prefix-length. The slash is required in the syntax.
ipv4-address **priority** *priority* **weight** *weight*	IPv4 Address of loopback interface. Associated with this locator address is a priority and weight that are used to define traffic policies when multiple RLOCs are defined for the same EID-prefix block. **Note** Lower priority locator takes preference.
ipv6-address	IPv6 Address of loopback interface.
map-request	Send map-request for LISP destination EID
native-forward	Natively forward packets that match this map-request.

Command Default

None.

Command Modes

LISP Instance Service (router-lisp-instance-service)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1c	This command was introduced.

Usage Guidelines

The first use of this command is to configure an Ingress Tunnel Router (ITR) with a static IPv4 or IPv6 EID-to-RLOC mapping relationship and its associated traffic policy. For each entry, a destination EID-prefix block and its associated locator, priority, and weight are entered. The value in the EID-prefix/prefix-length argument is the LISP EID-prefix block at the destination site. The locator is an IPv4 or IPv6 address of the remote site where the IPv4 or IPv6 EID-prefix can be reached. Associated with the locator address is a priority and weight that are used to define traffic policies when multiple RLOCs are defined for the same EID-prefix block.

```
device(config)#router lisp
device(config-router-lisp)#instance-id 3
device(config-router-lisp-inst)#service ipv4
device(config-router-lisp-inst-serv-ipv4)#map-cache 1.1.1.1/24 map-request
```

map-cache extranet

To install all configured extranet prefixes into map-cache, use the **map-cache extranet** command in the instance-service ipv4 or instance-service ipv6 mode.

map-cache extranet-registration

Command Default

None.

Command Modes

LISP Instance Service (router-lisp-instance-service)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1c	This command was introduced.

Usage Guidelines

To support inter-VRF communication, use the **map-cache extranet** command on the Map Server Map Resolver (MSMR). This command generates map requests for all fabric destinations. Use this command in the service ipv4 or service ipv6 mode under the extranet instance.

```
device(config)#router lisp
device(config-router-lisp)#instance-id 3
device(config-router-lisp-inst)#service ipv4
device(config-router-lisp-inst-serv-ipv4)#map-cache extranet-registration
```

prefix-list

To define a named LISP prefix set and to enter the LISP prefix-list configuration mode, use the **prefix-list** command in the Router LISP configuration mode. Use the **no** form of the command to remove the prefix list.

[**no**] **prefix-list** *prefix-list-name*

Syntax Description

prefix-list *prefix-list-name*	Specifies the prefix list to be used and enters the prefix-list configuration mode. Specifies IPv4 EID-prefixes or IPv6 EID-prefixes in the prefix-list mode.

Command Default

No prefix list is defined.

Command Modes

LISP (router-lisp)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1c	This command was introduced.

Usage Guidelines

Use the **prefix-list** command to configure an IPV4 or IPv6 prefix list. This command places the router in prefix-list configuration mode, in which you can define IPv4 prefix list, or IPv6 prefix list. Use the **exit-prefix-list** command to exit the prefix-list-configuration mode.

```
device(config)#router lisp
device(config-router-lisp)#prefix-list wired
device(config-router-prefix-list)#2001:193:168:1::/64
device(config-router-lisp-prefix-list)#192.168.0.0/16
device(config-router-lisp-prefix-list)#exit-prefix-list
```

route-import database

To configure the import of Routing Information Base (RIB) routes to define local endpoint identifier (EID) prefixes for database entries and associate them with a locator set, use the **route-import database** command in the instance service submode. To remove this configuration, use the **no** form of this command.

[**no**] **route-import database**
{**bgp** | **connected** | **eigrp** | **isis** | **maximum-prefix** | **ospf** | **ospfv3** | **rip** | **static**} {[**route-map**] **locator-set** *locator-set-name* **proxy**}

Syntax Description

bgp	Border Gateway Protocol. Imports RIB routes into LISP using BGP protocol.
connected	Connected routing protocol
eigrp	Enhanced Interior Gateway Routing Protocol. Imports RIB routes into LISP using EIGRP protocol.
isis	ISO IS-IS. Imports RIB routes into LISP using IS-IS protocol.
ospf	Open Shortest Path First
ospfv3	Open Shortest Path First version 3
maximum-prefix	Configures the maximum number of prefixes to pick up from the RIB.
rip	Routing Information Protocol
static	Defines static routes.
locator-set *locator-set-name*	Specifies the Locator Set to be used with created database mapping entries.
proxy	Enables the dynamic import of RIB route as proxy database mapping.

Command Default

None.

Command Modes

LISP Instance Service (router-lisp-instance-service)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1c	This command was introduced.

Usage Guidelines

Use the **route-import database** command with the **proxy** option to enable the dynamic import of RIB route as proxy database mapping. When RIB import is in use, the corresponding RIB map-cache import, using **route-import map-cache** command must also be configured, else the inbound site traffic will not pass the LISP eligibility check due to the presence of RIB route.

The following example shows how to configure the dynamic import of RIB route as proxy database:

```
device(config)#router lisp
device(config-router-lisp)#instance-id 3
```

```
device(config-router-lisp-inst)#service ipv4
device(config-router-lisp-inst-serv-ipv4)#eid-table default
device(config-router-lisp-inst-serv-ipv4)#database-mapping 193.168.0.0/16 locator-set RLOC
 proxy
device(config-router-lisp-inst-serv-ipv4)#route-import map-cache bgp 65002 route-map
map-cache-database
device(config-router-lisp-inst-serv-ipv4)#route-import database bgp 65002 locator-set RLOC
 proxy
```

service

The **service** command creates a configuration template for all instance-service instantiations of that particular service.

[**no**] **service** {**ipv4** | **ipv6** | **ethernet**}

Syntax Description

service ipv4	Enables Layer 3 network services for the IPv4 Address family.
service ipv6	Enables Layer 3 network services for the IPv6 Address family.
service ethernet	Enables Layer 2 network services.

Command Default

None.

Command Modes

LISP Instance (router-lisp-instance)

LISP (router-lisp)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1c	This command was introduced.

Usage Guidelines

The **service** command creates a service instance under the instance-id and enters the instance-service mode. You cannot confgure **service ethernet** for the same instance where **service ipv4** or **service ipv6** is configured.

Use the **no** form of the command to exit the service submode.

```
device(config)#router lisp
device(config-router-lisp)#instance-id 3
device(config-router-lisp-inst)#service ipv4
device(config-router-lisp-inst-serv-ipv4)#
```

```
device(config)#router lisp
device(config-router-lisp)#instance-id 5
device(config-router-lisp-inst)#service ethernet
device(config-router-lisp-inst-serv-ethernet)#
```

show lisp instance-id ipv4 database

To display the operational status of the IPv4 address family and the database mappings on the device, use the **show lisp instance-id ipv4 database** command in the privileged EXEC mode.

show lisp instance-id *instance-id* **ipv4 database**

Command Default

None.

Command Modes

Privileged Exec

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1c	This command was introduced.

Usage Guidelines

Use the command **show lisp instance-id *id* ipv4 database** to display the EID prefixes configured for a site. The following is a sample output:

```
device#show lisp instance-id 101 ipv4 database
LISP ETR IPv4 Mapping Database for EID-table vrf red (IID 101), LSBs: 0x1
Entries total 1, no-route 0, inactive 0

172.168.0.0/16, locator-set RLOC, proxy
  Locator          Pri/Wgt  Source     State
  100.110.110.110    1/100  cfg-intf   site-self, reachable

 device#

device#show lisp instance-id 101 ipv4
  Instance ID:                          101
  Router-lisp ID:                       0
  Locator table:                        default
  EID table:                            vrf red
  Ingress Tunnel Router (ITR):          disabled
  Egress Tunnel Router (ETR):           enabled
  Proxy-ITR Router (PITR):              enabled RLOCs: 100.110.110.110
  Proxy-ETR Router (PETR):              disabled
  NAT-traversal Router (NAT-RTR):       disabled
  Mobility First-Hop Router:            disabled
  Map Server (MS):                      enabled
  Map Resolver (MR):                    enabled
  Mr-use-petr:                          enabled
  Mr-use-petr locator set name:         site2
  Delegated Database Tree (DDT):        disabled
  Site Registration Limit:              0
  Map-Request source:                   derived from EID destination
  ITR Map-Resolver(s):                  100.77.77.77
                                        100.78.78.78
                                        100.110.110.110 prefix-list site2
  ETR Map-Server(s):                    100.77.77.77 (11:25:01)
                                        100.78.78.78 (11:25:01)
  xTR-ID:                               0xB843200A-0x4566BFC9-0xDAA75B2D-0x8FBE69B0
  site-ID:                              unspecified
  ITR local RLOC (last resort):         100.110.110.110
  ITR Solicit Map Request (SMR):        accept and process
    Max SMRs per map-cache entry:       8 more specifics
    Multiple SMR suppression time:      20 secs
```

```
 ETR accept mapping data:             disabled, verify disabled
 ETR map-cache TTL:                   1d00h
 Locator Status Algorithms:
   RLOC-probe algorithm:              disabled
   RLOC-probe on route change:        N/A (periodic probing disabled)
   RLOC-probe on member change:       disabled
   LSB reports:                       process
   IPv4 RLOC minimum mask length:     /0
   IPv6 RLOC minimum mask length:     /0
 Map-cache:
   Static mappings configured:        1
   Map-cache size/limit:              1/32768
   Imported route count/limit:        0/5000
   Map-cache activity check period:   60 secs
   Map-cache FIB updates:             established
   Persistent map-cache:              disabled
Database:
   Total database mapping size:       1
   static database size/limit:        1/65535
   dynamic database size/limit:       0/65535
   route-import database size/limit:  0/5000
   import-site-reg database size/limit0/65535
   proxy database size:               1
   Inactive (deconfig/away) size:     0
 Encapsulation type:                  vxlan
```

show lisp instance-id ipv6 database

To display the operational status of the IPv6 address family and the database mappings on the device, use the **show lisp instance-id ipv6 database** command in the privileged EXEC mode.

show lisp instance-id *instance-id* **ipv6 database**

Command Default

None.

Command Modes

Privileged Exec

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1c	This command was introduced.

Usage Guidelines

Use the command **show lisp instance-id *id* ipv6 database** to display the EID prefixes configured for a site. The following is a sample output:

```
device#show lisp instance-id 101 ipv6 database
LISP ETR IPv6 Mapping Database, LSBs: 0x1

EID-prefix: 2610:D0:1209::/48
  172.16.156.222, priority: 1, weight: 100, state: up, local

 device#
```

show lisp instance-id ipv4 map-cache

To display the IPv4 end point identifier (EID) to the Resource Locator (RLOC) cache mapping on an ITR, use the **show lisp instance-id ipv4 map-cache** command in the privileged Exec mode.

show lisp instance-id *instance-id* **ipv4 map-cache** [*destination-EID* | *destination-EID-prefix* | **detail**]

Syntax Description

destination-EID	(Optional) Specifies the IPv4 destination end point identifier (EID) for which the EID-to-RLOC mapping is displayed.
destination-EID-prefix	(Optional) Specifies the IPv4 destinationEID prefix (in the form of *a.b.c.d/nn*) for which to display the mapping.
detail	(Optional) Displays detailed EID-to-RLOC cache mapping information.

Command Default

None.

Command Modes

Privileged Exec

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1c	Introduced this command.

Usage Guidelines

This command is used to display the current dynamic and static IPv4 EID-to-RLOC map-cache entries. When no IPv4 EID or IPv4 EID prefix is specified, summary information is listed for all current dynamic and static IPv4 EID-to-RLOC map-cache entries. When an IPv4 EID or IPv4 EID prefix is included, information is listed for the longest-match lookup in the cache. When the detail option is used, detailed (rather than summary) information related to all current dynamic and static IPv4 EID-to-RLOC map-cache entries is displayed.

The following are sample outputs from the **show lisp instance-id ipv4 map-cache** commands:

```
device# show lisp instance-id 102 ipv4 map-cache
LISP IPv4 Mapping Cache for EID-table vrf blue (IID 102), 4008 entries

0.0.0.0/0, uptime: 2d14h, expires: never, via static-send-map-request
  Negative cache entry, action: send-map-request
128.0.0.0/3, uptime: 00:01:44, expires: 00:13:15, via map-reply, unknown-eid-forward
  PETR        Uptime    State      Pri/Wgt     Encap-IID
  55.55.55.1  13:32:40  up           1/100       103
  55.55.55.2  13:32:40  up           1/100       103
  55.55.55.3  13:32:40  up           1/100       103
  55.55.55.4  13:32:40  up           1/100       103
  55.55.55.5  13:32:40  up           5/100       103
  55.55.55.6  13:32:40  up           6/100       103
  55.55.55.7  13:32:40  up           7/100       103
  55.55.55.8  13:32:40  up           8/100       103
150.150.2.0/23, uptime: 11:47:25, expires: 00:06:30, via map-reply, unknown-eid-forward
  PETR        Uptime    State      Pri/Wgt     Encap-IID
  55.55.55.1  13:32:40  up           1/100       103
  55.55.55.2  13:32:40  up           1/100       103
  55.55.55.3  13:32:40  up           1/100       103
  55.55.55.4  13:32:40  up           1/100       103
  55.55.55.5  13:32:40  up           5/100       103
```

```
  55.55.55.6  13:32:40  up           6/100       103
  55.55.55.7  13:32:43  up           7/100       103
  55.55.55.8  13:32:43  up           8/100       103
150.150.4.0/22, uptime: 13:32:43, expires: 00:05:19, via map-reply, unknown-eid-forward
  PETR        Uptime    State      Pri/Wgt     Encap-IID
  55.55.55.1  13:32:43  up           1/100       103
  55.55.55.2  13:32:43  up           1/100       103
  55.55.55.3  13:32:43  up           1/100       103
  55.55.55.4  13:32:43  up           1/100       103
  55.55.55.5  13:32:43  up           5/100       103
  55.55.55.6  13:32:43  up           6/100       103
  55.55.55.7  13:32:43  up           7/100       103
  55.55.55.8  13:32:43  up           8/100       103
150.150.8.0/21, uptime: 13:32:35, expires: 00:05:27, via map-reply, unknown-eid-forward
  PETR        Uptime    State      Pri/Wgt     Encap-IID
 55.55.55.1  13:32:43  up           1/100       103
  55.55.55.2  13:32:43  up           1/100       103
  55.55.55.3  13:32:43  up           1/100       103
  55.55.55.4  13:32:43  up           1/100       103
  55.55.55.5  13:32:43  up           5/100       103
  55.55.55.6  13:32:43  up           6/100       103
  55.55.55.7  13:32:43  up           7/100       103
  55.55.55.8  13:32:45  up           8/100       103
171.171.0.0/16, uptime: 2d14h, expires: never, via dynamic-EID, send-map-request
  Negative cache entry, action: send-map-request
172.172.0.0/16, uptime: 2d14h, expires: never, via dynamic-EID, send-map-request
  Negative cache entry, action: send-map-request
178.168.2.1/32, uptime: 2d14h, expires: 09:27:13, via map-reply, complete
  Locator     Uptime    State      Pri/Wgt     Encap-IID
  11.11.11.1  2d14h     up           1/100       -
178.168.2.2/32, uptime: 2d14h, expires: 09:27:13, via map-reply, complete
  Locator     Uptime    State      Pri/Wgt     Encap-IID
  11.11.11.1  2d14h     up           1/100       -
178.168.2.3/32, uptime: 2d14h, expires: 09:27:13, via map-reply, complete
  Locator     Uptime    State      Pri/Wgt     Encap-IID
  11.11.11.1  2d14h     up           1/100       -
178.168.2.4/32, uptime: 2d14h, expires: 09:27:13, via map-reply, complete
  Locator     Uptime    State      Pri/Wgt     Encap-IID
  11.11.11.1  2d14h     up           1/100       -
178.168.2.5/32, uptime: 2d14h, expires: 09:27:13, via map-reply, complete
  Locator     Uptime    State      Pri/Wgt     Encap-IID
  11.11.11.1  2d14h     up           1/100       -
178.168.2.6/32, uptime: 2d14h, expires: 09:27:13, via map-reply, complete
  Locator     Uptime    State      Pri/Wgt     Encap-IID
```

```
device#show lisp instance-id 102 ipv4 map-cache detail
LISP IPv4 Mapping Cache for EID-table vrf blue (IID 102), 4008 entries

0.0.0.0/0, uptime: 2d15h, expires: never, via static-send-map-request
  Sources: static-send-map-request
  State: send-map-request, last modified: 2d15h, map-source: local
  Exempt, Packets out: 30531(17585856 bytes) (~ 00:01:36 ago)
  Configured as EID address space
  Negative cache entry, action: send-map-request
128.0.0.0/3, uptime: 00:02:02, expires: 00:12:57, via map-reply, unknown-eid-forward
  Sources: map-reply
  State: unknown-eid-forward, last modified: 00:02:02, map-source: local
  Active, Packets out: 9(5184 bytes) (~ 00:00:36 ago)
  PETR        Uptime    State      Pri/Wgt     Encap-IID
  55.55.55.1  13:32:58  up           1/100       103
  55.55.55.2  13:32:58  up           1/100       103
  55.55.55.3  13:32:58  up           1/100       103
  55.55.55.4  13:32:58  up           1/100       103
  55.55.55.5  13:32:58  up           5/100       103
  55.55.55.6  13:32:58  up           6/100       103
```

```
  55.55.55.7  13:32:58  up           7/100       103
  55.55.55.8  13:32:58  up           8/100       103
150.150.2.0/23, uptime: 11:47:43, expires: 00:06:12, via map-reply, unknown-eid-forward
  Sources: map-reply
  State: unknown-eid-forward, last modified: 11:47:44, map-source: local
  Active, Packets out: 4243(2443968 bytes) (~ 00:00:38 ago)
  PETR        Uptime    State      Pri/Wgt     Encap-IID
  55.55.55.1  13:33:00  up           1/100       103
  55.55.55.2  13:33:00  up           1/100       103
  55.55.55.3  13:33:00  up           1/100       103
  55.55.55.4  13:33:00  up           1/100       103
  55.55.55.5  13:33:00  up           5/100       103
  55.55.55.6  13:33:00  up           6/100       103
  55.55.55.7  13:33:00  up           7/100       103
  55.55.55.8  13:33:00  up           8/100       103
150.150.4.0/22, uptime: 13:33:00, expires: 00:05:02, via map-reply, unknown-eid-forward
  Sources: map-reply
  State: unknown-eid-forward, last modified: 13:33:00, map-source: local
  Active, Packets out: 4874(2807424 bytes) (~ 00:00:38 ago)
  PETR        Uptime    State      Pri/Wgt     Encap-IID
  55.55.55.1  13:33:00  up           1/100       103
  55.55.55.2  13:33:00  up           1/100       103
  55.55.55.3  13:33:00  up           1/100       103
  55.55.55.4  13:33:00  up           1/100       103
 55.55.55.5  13:33:00  up           5/100       103
  55.55.55.6  13:33:00  up           6/100       103
  55.55.55.7  13:33:01  up           7/100       103
  55.55.55.8  13:33:01  up           8/100       103
150.150.8.0/21, uptime: 13:32:53, expires: 00:05:09, via map-reply, unknown-eid-forward
  Sources: map-reply
  State: unknown-eid-forward, last modified: 13:32:53, map-source: local
  Active, Packets out: 4874(2807424 bytes) (~ 00:00:39 ago)
  PETR        Uptime    State      Pri/Wgt     Encap-IID
  55.55.55.1  13:33:01  up           1/100       103
  55.55.55.2  13:33:01  up           1/100       103
  55.55.55.3  13:33:01  up           1/100       103
  55.55.55.4  13:33:01  up           1/100       103
  55.55.55.5  13:33:01  up           5/100       103
  55.55.55.6  13:33:01  up           6/100       103
  55.55.55.7  13:33:01  up           7/100       103
  55.55.55.8  13:33:01  up           8/100       103
171.171.0.0/16, uptime: 2d15h, expires: never, via dynamic-EID, send-map-request
  Sources: NONE
  State: send-map-request, last modified: 2d15h, map-source: local
  Exempt, Packets out: 2(1152 bytes) (~ 2d14h ago)
  Configured as EID address space
  Configured as dynamic-EID address space
  Encapsulating dynamic-EID traffic
  Negative cache entry, action: send-map-request
172.172.0.0/16, uptime: 2d15h, expires: never, via dynamic-EID, send-map-request
  Sources: NONE
  State: send-map-request, last modified: 2d15h, map-source: local
  Exempt, Packets out: 2(1152 bytes) (~ 2d14h ago)
  Configured as EID address space
  Configured as dynamic-EID address space
  Encapsulating dynamic-EID traffic
  Negative cache entry, action: send-map-request
178.168.2.1/32, uptime: 2d14h, expires: 09:26:55, via map-reply, complete
  Sources: map-reply
  State: complete, last modified: 2d14h, map-source: 48.1.1.4
  Active, Packets out: 22513(12967488 bytes) (~ 00:00:41 ago)
  Locator     Uptime    State      Pri/Wgt     Encap-IID
  11.11.11.1  2d14h     up           1/100       -
    Last up-down state change:         2d14h, state change count: 1
```

```
    Last route reachability change:    2d14h, state change count: 1
    Last priority / weight change:     never/never
    RLOC-probing loc-status algorithm:
      Last RLOC-probe sent:            2d14h (rtt 92ms)
178.168.2.2/32, uptime: 2d14h, expires: 09:26:55, via map-reply, complete
  Sources: map-reply
  State: complete, last modified: 2d14h, map-source: 48.1.1.4
  Active, Packets out: 22513(12967488 bytes) (~ 00:00:45 ago)
  Locator     Uptime    State      Pri/Wgt     Encap-IID
  11.11.11.1  2d14h     up           1/100       -
    Last up-down state change:         2d14h, state change count: 1
    Last route reachability change:    2d14h, state change count: 1
    Last priority / weight change:     never/never
    RLOC-probing loc-status algorithm:
      Last RLOC-probe sent:            2d14h (rtt 91ms)
178.168.2.3/32, uptime: 2d14h, expires: 09:26:51, via map-reply, complete
  Sources: map-reply
  State: complete, last modified: 2d14h, map-source: 48.1.1.4
  Active, Packets out: 22513(12967488 bytes) (~ 00:00:45 ago)
  Locator     Uptime    State      Pri/Wgt     Encap-IID
  11.11.11.1  2d14h     up           1/100       -
    Last up-down state change:         2d14h, state change count: 1
    Last route reachability change:    2d14h, state change count: 1
    Last priority / weight change:     never/never
    RLOC-probing loc-status algorithm:
      Last RLOC-probe sent:            2d14h (rtt 91ms)
178.168.2.4/32, uptime: 2d14h, expires: 09:26:51, via map-reply, complete
  Sources: map-reply
  State: complete, last modified: 2d14h, map-source: 48.1.1.4
```

```
device#show lisp instance-id 102 ipv4 map-cache 178.168.2.3/32
LISP IPv4 Mapping Cache for EID-table vrf blue (IID 102), 4008 entries

178.168.2.3/32, uptime: 2d14h, expires: 09:26:25, via map-reply, complete
  Sources: map-reply
  State: complete, last modified: 2d14h, map-source: 48.1.1.4
  Active, Packets out: 22519(12970944 bytes) (~ 00:00:11 ago)
  Locator     Uptime    State      Pri/Wgt     Encap-IID
  11.11.11.1  2d14h     up           1/100       -
    Last up-down state change:         2d14h, state change count: 1
    Last route reachability change:    2d14h, state change count: 1
    Last priority / weight change:     never/never
    RLOC-probing loc-status algorithm:
      Last RLOC-probe sent:            2d14h (rtt 91ms)
```

```
device#show lisp instance-id 102 ipv4 map-cache 178.168.2.3
LISP IPv4 Mapping Cache for EID-table vrf blue (IID 102), 4008 entries

178.168.2.3/32, uptime: 2d14h, expires: 09:26:14, via map-reply, complete
  Sources: map-reply
  State: complete, last modified: 2d14h, map-source: 48.1.1.4
  Active, Packets out: 22519(12970944 bytes) (~ 00:00:22 ago)
  Locator     Uptime    State      Pri/Wgt     Encap-IID
  11.11.11.1  2d14h     up           1/100       -
    Last up-down state change:         2d14h, state change count: 1
    Last route reachability change:    2d14h, state change count: 1
    Last priority / weight change:     never/never
    RLOC-probing loc-status algorithm:
      Last RLOC-probe sent:            2d14h (rtt 91ms)
OTT-LISP-C3K-4-xTR2#show lisp instance-id 102 sta
OTT-LISP-C3K-4-xTR2#show lisp instance-id 102 stat
OTT-LISP-C3K-4-xTR2#show lisp instance-id 102 ipv4 stat
OTT-LISP-C3K-4-xTR2#show lisp instance-id 102 ipv4 statistics
LISP EID Statistics for instance ID 102 - last cleared: never
Control Packets:
```

```
  Map-Requests in/out:                              5911/66032
    Map-Request receive rate (5 sec/1 min/5 min):   0.00/ 0.00/ 0.00
    Encapsulated Map-Requests in/out:               0/60600
    RLOC-probe Map-Requests in/out:                 5911/5432
    SMR-based Map-Requests in/out:                  0/0
    Extranet SMR cross-IID Map-Requests in:         0
    Map-Requests expired on-queue/no-reply          0/0
    Map-Resolver Map-Requests forwarded:            0
    Map-Server Map-Requests forwarded:              0
  Map-Reply records in/out:                         64815/5911
    Authoritative records in/out:                   12696/5911
    Non-authoritative records in/out:               52119/0
    Negative records in/out:                        8000/0
    RLOC-probe records in/out:                      4696/5911
    Map-Server Proxy-Reply records out:             0
  WLC Map-Subscribe records in/out:                 0/4
    Map-Subscribe failures in/out:                  0/0
  WLC Map-Unsubscribe records in/out:               0/0
    Map-Unsubscribe failures in/out:                0/0
  Map-Register records in/out:                      0/8310
    Map-Register receive rate (5 sec/1 min/5 min):  0.00/ 0.00/ 0.00
    Map-Server AF disabled:                         0
    Authentication failures:                        0
  WLC Map-Register records in/out:                  0/0
    WLC AP Map-Register in/out:                     0/0
    WLC Client Map-Register in/out:                 0/0
    WLC Map-Register failures in/out:               0/0
  Map-Notify records in/out:                        20554/0
    Authentication failures:                        0
  WLC Map-Notify records in/out:                    0/0
    WLC AP Map-Notify in/out:                       0/0
    WLC Client Map-Notify in/out:                   0/0
    WLC Map-Notify failures in/out:                 0/0
  Publish-Subscribe in/out:
    Subscription Request records in/out:            0/6
    Subscription Request failures in/out:           0/0
    Subscription Status records in/out:             4/0
      End of Publication records in/out:            4/0
      Subscription rejected records in/out:         0/0
      Subscription removed records in/out:          0/0
    Subscription Status failures in/out:            0/0
    Solicit Subscription records in/out:            0/0
    Solicit Subscription failures in/out:           0/0
    Publication records in/out:                     0/0
    Publication failures in/out:                    0/0
Errors:
  Mapping record TTL alerts:                        0
  Map-Request invalid source rloc drops:            0
  Map-Register invalid source rloc drops:           0
  DDT Requests failed:                              0
  DDT ITR Map-Requests dropped:                     0 (nonce-collision: 0, bad-xTR-nonce:
0)
Cache Related:
  Cache entries created/deleted:                    200103/196095
  NSF CEF replay entry count                        0
  Number of EID-prefixes in map-cache:              4008
  Number of rejected EID-prefixes due to limit :    0
  Number of negative entries in map-cache:          8
  Total number of RLOCs in map-cache:               4000
  Average RLOCs per EID-prefix:                     1
Forwarding:
  Number of data signals processed:                 199173 (+ dropped 5474)
  Number of reachability reports:                   0 (+ dropped 0)
  Number of SMR signals dropped:                    0
```

```
ITR Map-Resolvers:
  Map-Resolver         LastReply  Metric ReqsSent Positive Negative No-Reply    AvgRTT(5
sec/1 min/5 min)
  44.44.44.44          00:03:11        6    62253    19675     8000        0    0.00/
0.00/10.00
  66.66.66.66          never     Unreach        0        0        0        0    0.00/ 0.00/
 0.00
ETR Map-Servers:
  Map-Server           AvgRTT(5 sec/1 min/5 min)
  44.44.44.44          0.00/ 0.00/ 0.00
  66.66.66.66          0.00/ 0.00/ 0.00
LISP RLOC Statistics - last cleared: never
Control Packets:
  RTR Map-Requests forwarded:                     0
  RTR Map-Notifies forwarded:                     0
  DDT-Map-Requests in/out:                        0/0
  DDT-Map-Referrals in/out:                       0/0
Errors:
  Map-Request format errors:                      0
  Map-Reply format errors:                        0
  Map-Referral format errors:                     0
LISP Miscellaneous Statistics - last cleared: never
Errors:
  Invalid IP version drops:                       0
  Invalid IP header drops:                        0
  Invalid IP proto field drops:                   0
  Invalid packet size drops:                      0
  Invalid LISP control port drops:                0
  Invalid LISP checksum drops:                    0
  Unsupported LISP packet type drops:             0
  Unknown packet drops:                           0
```

show lisp instance-id ipv6 map-cache

To display the IPv6 end point identifier (EID) to the Resource Locator (RLOC) cache mapping on an ITR, use the **show lisp instance-id ipv6 map-cache** command in the privileged EXEC mode.

show lisp instance-id *instance-id* **ipv6 map-cache** [*destination-EID* | *destination-EID-prefix* | **detail**]

Syntax Description

destination-EID	(Optional) Specifies the IPv4 destination end point identifier (EID) for which the EID-to-RLOC mapping is displayed.
destination-EID-prefix	(Optional) Specifies the IPv4 destination EID prefix (in the form of *a.b.c.d/nn*) for which to display the mapping.
detail	(Optional) Displays detailed EID-to-RLOC cache mapping information.

Command Default

None.

Command Modes

Privileged Exec

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1c	Introduced this command.

Usage Guidelines

This command is used to display the current dynamic and static IPv6 EID-to-RLOC map-cache entries. When no IPv6 EID or IPv6 EID prefix is specified, summary information is listed for all current dynamic and static IPv4 EID-to-RLOC map-cache entries. When an IPv6 EID or IPv6 EID prefix is included, information is listed for the longest-match lookup in the cache. When the detail option is used, detailed (rather than summary) information related to all current dynamic and static IPv6 EID-to-RLOC map-cache entries is displayed.

The following is a sample output from the **show lisp instance-id ipv6 map-cache** command:

```
device# show lisp instance-id 101 ipv6 map-cache
LISP IPv6 Mapping Cache, 2 entries

::/0, uptime: 00:00:26, expires: never, via static
  Negative cache entry, action: send-map-request
2001:DB8:AB::/48, uptime: 00:00:04, expires: 23:59:53, via map-reply, complete
  Locator   Uptime    State      Pri/Wgt
  10.0.0.6  00:00:04  up           1/100
```

The following sample output from the **show lisp instance-id x ipv6 map-cache detail** command displays a detailed list of current dynamic and static IPv6 EID-to-RLOC map-cache entries:

```
device#show lisp instance-id 101 ipv6 map-cache detail
LISP IPv6 Mapping Cache, 2 entries

::/0, uptime: 00:00:52, expires: never, via static
  State: send-map-request, last modified: 00:00:52, map-source: local
  Idle, Packets out: 0
  Negative cache entry, action: send-map-request
2001:DB8:AB::/48, uptime: 00:00:30, expires: 23:59:27, via map-reply, complete
  State: complete, last modified: 00:00:30, map-source: 10.0.0.6
  Active, Packets out: 0
  Locator   Uptime    State      Pri/Wgt
```

```
  10.0.0.6  00:00:30  up           1/100
    Last up-down state change:         never, state change count: 0
    Last priority / weight change:     never/never
    RLOC-probing loc-status algorithm:
      Last RLOC-probe sent:            never
```

The following sample output from the show ipv6 lisp map-cache command with a specific IPv6 EID prefix displays detailed information associated with that IPv6 EID prefix entry.

```
device#show lisp instance-id 101 ipv6 map-cache 2001:DB8:AB::/48
LISP IPv6 Mapping Cache, 2 entries

2001:DB8:AB::/48, uptime: 00:01:02, expires: 23:58:54, via map-reply, complete
  State: complete, last modified: 00:01:02, map-source: 10.0.0.6
  Active, Packets out: 0
  Locator   Uptime    State      Pri/Wgt
  10.0.0.6  00:01:02  up           1/100
    Last up-down state change:         never, state change count: 0
    Last priority / weight change:     never/never
    RLOC-probing loc-status algorithm:
        Last RLOC-probe sent:            never
```

show lisp instance-id ipv4 server

To display the LISP site registration information, use the **show lisp instance-id ipv4 server** command in the privileged EXEC mode.

show lisp instance-id *instance-id***ipv4 server** [*EID-address* | *EID-prefix* | **detail** | **name** | **rloc** | **summary**]

Syntax Description

EID-address	(Optional) Displays site registration information for this end point.
EID-prefix	(Optional) Displays site registration information for this IPv4 EID prefix.
detail	(Optional) Displays a detailed site information.
name	(Optional) Displays the site registration information for the named site.
rloc	(Optional) Displays the RLOC-EID instance membership details.
summary	(Optional) Displays summary information for each site.

Command Default

None.

Command Modes

Privileged Exec

Command History

Release	Modification
	This command was introduced.

Usage Guidelines

When a host is detected by the tunnel router (xTR), it registers the host with the map server (MS). Use the **show lisp instance-id x ipv4 server** command to see the site registration details. TCP registrations display the port number, whereas UDP registration do not display port number. The port number is 4342 by default fir UDP registration.

The following are sample outputs of the command :

```
device# show lisp instance-id 100 ipv4 server
LISP Site Registration Information
* = Some locators are down or unreachable
# = Some registrations are sourced by reliable transport

Site Name      Last      Up     Who Last             Inst     EID Prefix
               Register         Registered           ID
XTR            00:03:22  yes*#  172.16.1.4:64200     100      101.1.0.0/16
               00:03:16  yes#   172.16.1.3:19881     100      101.1.1.1/32
```

```
device# show lisp instance-id 100 ipv4 server 101.1.0.0/16
LISP Site Registration Information

Site name: XTR
Allowed configured locators: any
Requested EID-prefix:

  EID-prefix: 101.1.0.0/16 instance-id 100
    First registered:     00:04:24
    Last registered:      00:04:20
```

```
    Routing table tag:    0
    Origin:               Configuration, accepting more specifics
    Merge active:         No
    Proxy reply:          No
    TTL:                  1d00h
    State:                complete
    Registration errors:
      Authentication failures:   0
      Allowed locators mismatch: 0
    ETR 172.16.1.4:64200, last registered 00:04:20, no proxy-reply, map-notify
                        TTL 1d00h, no merge, hash-function sha1, nonce 0xC1ED8EE1-0x553D05D4

                           state complete, no security-capability
                           xTR-ID 0x46B2F3A5-0x19B0A3C5-0x67055A44-0xF5BF3FBB
                           site-ID unspecified
                           sourced by reliable transport
      Locator     Local  State      Pri/Wgt  Scope
      172.16.1.4  yes    admin-down 255/100  IPv4 none
```

The following is an ouput that shows an UDP registration (without port number):

```
device# show lisp instance-id 100 ipv4 server 101.1.1.1/32
LISP Site Registration Information

Site name: XTR
Allowed configured locators: any
Requested EID-prefix:

  EID-prefix: 101.1.1.1/32 instance-id 100
    First registered:     00:00:08
    Last registered:      00:00:04
    Routing table tag:    0
    Origin:               Dynamic, more specific of 101.1.0.0/16
    Merge active:         No
    Proxy reply:          No
    TTL:                  1d00h
    State:                complete
    Registration errors:
      Authentication failures:   0
      Allowed locators mismatch: 0
    ETR 172.16.1.3:46245, last registered 00:00:04, no proxy-reply, map-notify
                        TTL 1d00h, no merge, hash-function sha1, nonce 0x1769BD91-0x06E10A06

                           state complete, no security-capability
                           xTR-ID 0x4F5F0056-0xAE270416-0x360B42D6-0x6FCD3F5B
                           site-ID unspecified
                           sourced by reliable transport
      Locator     Local  State      Pri/Wgt  Scope
      172.16.1.3  yes    up         100/100  IPv4 none
    ETR 172.16.1.3, last registered 00:00:08, no proxy-reply, map-notify
                    TTL 1d00h, no merge, hash-function sha1, nonce 0x1769BD91-0x06E10A06
                    state complete, no security-capability
                    xTR-ID 0x4F5F0056-0xAE270416-0x360B42D6-0x6FCD3F5B
                    site-ID unspecified
      Locator     Local  State      Pri/Wgt  Scope
      172.16.1.3  yes    up         100/100  IPv4 none
```

show lisp instance-id ipv6 server

To display the LISP site registration information, use the **show lisp instance-id ipv6 server** command in the privileged EXEC mode.

show lisp instance-id *instance-id***ipv6 server** [*EID-address* | *EID-prefix* | **detail** | **name** | **rloc** | **summary**]

Syntax Description

EID-address	(Optional) Displays site registration information for this end point.
EID-prefix	(Optional) Displays site registration information for this IPv6 EID prefix.
detail	(Optional) Displays a detailed site information.
name	(Optional) Displays the site registration information for the named site.
rloc	(Optional) Displays the RLOC-EID instance membership details.
summary	(Optional) Displays summary information for each site.

Command Default

None.

Command Modes

Privileged Exec

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1c	This command was introduced.

Usage Guidelines

When a host is detected by the tunnel router (xTR), it registers the host with the map server (MS). Use the **show lisp instance-id ipv6 server** command to see the site registration details.

show lisp instance-id ipv4 statistics

To display Locator/ID Separation Protocol (LISP) IPv4 address-family packet count statistics, use the **show lisp instance-id ipv4 statistics** command in the privileged EXEC mode.

show lisp instance-id *instance-id* **ipv4 statistics**

Command Default

None.

Command Modes

Privileged Exec

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1c	This command was introduced.

Usage Guidelines

This command is used to display IPv4 LISP statistics related to packet encapsulations, de-encapsulations, map requests, map replies, map registers, and other LISP-related packets.

The following are sample outputs of the command :

```
device# show lisp instance-id 100 ipv4 statistics
```

show lisp instance-id ipv6 statistics

To display Locator/ID Separation Protocol (LISP) IPv6 address-family packet count statistics, use the **show lisp instance-id ipv6 statistics** command in the privileged EXEC mode.

show lisp instance-id *instance-id* **ipv6 statistics**

Command Default

None.

Command Modes

Privileged Exec

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1c	This command was introduced.

Usage Guidelines

This command is used to display IPv4 LISP statistics related to packet encapsulations, de-encapsulations, map requests, map replies, map registers, and other LISP-related packets.

The following are sample outputs of the command :

```
device# show lisp instance-id 100 ipv6 statistics
```

show lisp prefix-list

To display the LISP prefix-list information, use the **show lisp prefix-list** command in the privileged EXEC mode.

show lisp prefix-list [*name-prefix-list*]

Syntax Description

name-prefix-list	(Optional) Specifies the prefix-list whose information is displayed.

Command Default

None.

Command Modes

Privileged Exec

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1c	This command was introduced.

Usage Guidelines

The following is a sample output from the **show lisp prefix-list** command:

```
device# show lisp prefix-list
Lisp Prefix List information for router lisp 0

Prefix List: set
    Number of entries: 1
    Entries:
 1.2.3.4/16
     Sources: static
```

show lisp session

To display the current list of reliable transport sessions in the fabric, use the **show lisp session** command in the privileged EXEC mode.

show lisp session [**all** | **established**]

Syntax Description

all	(Optional) Displays transport session inforamtion for all the sessions.
established	(Optional) Displays transport session information for established connections.

Command Default

None.

Command Modes

Privileged Exec

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1c	This command was introduced.

Usage Guidelines

The **show lisp session** command displays only those sessions that are in Up or Down state. Use the **show lisp session all** command to see all sessions in any state.

The following is a sample output of the command **show lisp session** on an MSMR:

```
device# show lisp session
Sessions for VRF default, total: 4, established: 2
Peer                          State      Up/Down        In/Out    Users
172.16.1.3:22667              Up         00:00:52        4/8      2
172.16.1.4:18904              Up         00:22:15        5/13     1

device# show lisp session all
Sessions for VRF default, total: 4, established: 2
Peer                          State      Up/Down        In/Out    Users
172.16.1.3                    Listening  never           0/0      0
172.16.1.3:22667              Up         00:01:13        4/8      2
172.16.1.4                    Listening  never           0/0      0
172.16.1.4:18904              Up         00:22:36        5/13     1
```

use-petr

To configure a router to use an IPv4 or IPv6 Locator/ID Separation Protocol (LISP) Proxy Egress Tunnel Router (PETR), use the **use-petr** command in LISP Instance configuration mode or LISP Instance Service configuration mode. To remove the use of a LISP PETR, use the **no** form of this command.

[**no**] **use-petr** *locator-address*[**priority** *priority* **weight** *weight*]

Syntax Description

locator-address	The name of locator-set that is set as default.
priority *priority*	(Optional) Specifies the priority (value between 0 and 255) assigned to this PETR. A lower value indicates a higher priority.
weight *weight*	(Optional) Specifies the percentage of traffic to be load-shared (value between 0 and 100).

Command Default

The router does not use PETR services.

Command Modes

LISP Service (router-lisp-service)

LISP Instance-Service (router-lisp-instance-service)

Command History

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1c	This command was introduced.

Usage Guidelines

Use the **use-petr** command to enable an Ingress Tunnel Router (ITR) or Proxy Ingress Tunnel Router (PITR) to use IPv4 Proxy Egress Tunnel Router (PETR) services. When the use of PETR services is enabled, instead of natively forwarding LISP endpoint identifier (EID) (source) packets destined to non-LISP sites, these packets are LISP-encapsulated and forwarded to the PETR. Upon receiving these packets, the PETR decapsulates them and then forwards them natively toward the non-LISP destination.

Do not use **use-petr** command in Service-Ethernet configuration mode.

PETR services may be necessary in several cases:

1. By default when a LISP site forwards packets to a non-LISP site natively (not LISP encapsulated), the source IP address of the packet is that of an EID. When the provider side of the access network is configured with strict unicast reverse path forwarding (uRPF) or an anti-spoofing access list, it may consider these packets to be spoofed and drop them since EIDs are not advertised in the provider core network. In this case, instead of natively forwarding packets destined to non-LISP sites, the ITR encapsulates these packets using its site locator(s) as the source address and the PETR as the destination address.

Note The use of the **use-petr** command does not change LISP-to-LISP or non-LISP-to-non-LISP forwarding behavior. LISP EID packets destined for LISP sites will follow normal LISP forwarding processes and be sent directly to the destination ETR as normal. Non-LISP-to-non-LISP packets are never candidates for LISP encapsulation and are always forwarded natively according to normal processes.

2. When a LISP IPv6 (EID) site needs to connect to a non-LISP IPv6 site and the ITR locators or some portion of the intermediate network does not support IPv6 (it is IPv4 only), the PETR can be used to traverse (hop over) the address family incompatibility, assuming that the PETR has both IPv4 and IPv6 connectivity. The ITR in this case can LISP-encapsulate the IPv6 EIDs with IPv4 locators destined for the PETR, which de-encapsulates the packets and forwards them natively to the non-LISP IPv6 site over its IPv6 connection. In this case, the use of the PETR effectively allows the LISP site packets to traverse the IPv4 portion of network using the LISP mixed protocol encapsulation support.

Examples

The following example shows how to configure an ITR to use the PETR with the IPv4 locator of 10.1.1.1. In this case, LISP site IPv4 EIDs destined to non-LISP IPv4 sites are encapsulated in an IPv4 LISP header destined to the PETR located at 10.1.1.1:

```
device(config)# router lisp
device(config-router-lisp)#service ipv4
device(config-router-lisp-serv-ipv4)# use-petr 10.1.1.1
```

The following example configures an ITR to use two PETRs: one has an IPv4 locator of 10.1.1.1 and is configured as the primary PETR (priority 1 weight 100), and the other has an IPv4 locator of 10.1.2.1 and is configured as the secondary PETR (priority 2 weight 100). In this case, LISP site IPv4 EIDs destined to non-LISP IPv4 sites will be encapsulated in an IPv4 LISP header to the primary PETR located at 10.1.1.1 unless it fails, in which case the secondary will be used.

```
Router(config-router-lisp-serv-ipv4)# use-petr 10.1.1.1 priority 1 weight 100
Router(config-router-lisp-serv-ipv4)# use-petr 10.1.2.1 priority 2 weight 100
```

PART II

Cisco TrustSec

- Cisco TrustSec Commands, on page 69

Cisco TrustSec Commands

- cts authorization list, on page 71
- cts change-password, on page 72
- cts credentials, on page 73
- cts refresh, on page 75
- cts rekey, on page 77
- cts role-based enforcement, on page 78
- cts role-based l2-vrf, on page 79
- cts role-based monitor, on page 81
- cts role-based permissions, on page 82
- cts role-based sgt-caching, on page 84
- cts role-based sgt-map, on page 85
- cts sxp connection peer, on page 87
- cts sxp default password, on page 90
- cts sxp default source-ip, on page 92
- cts sxp filter-enable, on page 94
- cts sxp filter-group, on page 95
- cts sxp filter-list, on page 97
- cts sxp log binding-changes, on page 99
- cts sxp reconciliation period, on page 100
- cts sxp retry period, on page 101
- propagate sgt (cts manual), on page 102
- sap mode-list (cts manual), on page 104
- show cts credentials, on page 106
- show cts interface, on page 107
- show cts role-based counters, on page 109
- show cts role-based permissions, on page 111
- show cts server-list, on page 113
- show cts sxp, on page 115
- show platform hardware fed switch active fwd-asic resource tcam utilization , on page 118
- show platform hardware fed switch active sgacl resource usage, on page 120
- show platform software classification switch active F0 class-group-manager class-group client acl all, on page 121
- show platform software cts forwarding-manager switch active F0 port, on page 122

- show platform software cts forwarding-manager switch active F0, on page 126
- show platform software cts forwarding-manager switch active F0 permissions, on page 127
- show platform software fed switch active acl counters hardware | inc SGACL , on page 129
- show platform software fed switch active acl usage , on page 130
- show platform software fed switch active ifm mappings , on page 131
- show platform software fed switch active ip route , on page 133
- show platform software fed switch active sgacl detail , on page 135
- show platform software fed switch active sgacl port , on page 136
- show platform software fed switch active sgacl vlan , on page 138
- show platform software status control-processor brief, on page 139
- show monitor capture <name> buffer, on page 140

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.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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:

```
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

Command	Description
show cts server-list	Displays RADIUS server configurations.

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	UPD 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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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 ffef
```

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.

cts 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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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 pacssword 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

Command	Description
clear cts credentials	Clears the Cisco TrustSec device ID and password.
show cts credentials	Displays the state of the current Cisco TrustSec device ID and password.
show cts keystore	Displays contents of the hardware and software keystores.

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.

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

Syntax Description

environment-data	Refreshes environment data.
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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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
```

Related Commands

Command	Description
clear cts policy	Clears all Cisco TrustSec policies, or by the peer ID or SGT.
show cts policy peer	Displays peer authorization policy for all or specific TrustSec peers.

cts rekey

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

cts 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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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

Command	Description
sap mode-list (cts manual)	Configures Cisco TrustSec SAP for manual mode.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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*} [{**,**}] [{**-**}]
no 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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The *vlan-list* argument can be a single VLAN ID, a list of comma-separated VLAN IDs, or hyphen-separated VLAN ID ranges.

The **all** keyword is equivalent to the full range of VLANs supported by the network device. The **all** keyword is not preserved in the nonvolatile generation (NVGEN) process.

If the **cts role-based l2-vrf** command is issued more than once for the same VRF, each successive command entered adds the VLAN IDs to the specified VRF.

The VRF assignments configured by the **cts role-based l2-vrf** command are active as long as a VLAN remains a Layer 2 VLAN. The IP–SGT bindings learned while a VRF assignment is active are also added to the Forwarding Information Base (FIB) table associated with the VRF and the IP protocol version. If an Switched Virtual Interface (SVI) becomes active for a VLAN, the VRF-to-VLAN assignment becomes inactive and all bindings learned on the VLAN are moved to the FIB table associated with the VRF of the SVI.

Use the **interface vlan** command to configure an SVI interface, and the **vrf forwarding** command to associate a VRF instance to the interface.

The VRF-to-VLAN assignment is retained even when the assignment becomes inactive. It is reactivated when the SVI is removed or when the SVI IP address is changed. When reactivated, the IP–SGT bindings are moved back from the FIB table associated with the VRF of the SVI to the FIB table associated with the VRF assigned by the **cts role-based l2-vrf** command.

The following example shows how to select a list of VLANS to be assigned to a VRF instance:

```
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

Command	Description
interface vlan	Configures a VLAN interface.
vrf forwarding	Associates a VRF instance or a virtual network with an interface or subinterface.
show cts role-based permissions	Displays the SGACL permission list.

cts role-based monitor

To enable role-based (security-group) access list monitoring, use the **cts role-based monitor** command in global configuration mode. To remove role-based access list monitoring, use the **no** form of this command.

cts role-based monitor {**all** | **permissions** {**default** [{**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

all	Monitors permissions for all source tags to all destination tags.
permissions	Monitors permissions from a source tags to a destination tags.
default	Monitors the default permission list.
ipv4	(Optional) Specifies the IPv4 protocol.
ipv6	(Optional) Specifies the IPv6 protocol.
from	Specifies the source group tag for filtered traffic.
sgt	Security Group Tag (SGT). Valid values are from 2 to 65519.
unknown	Specifies an unknown source or destination group tag (DST).

Command Default

Role-based access control monitoring is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Use the **cts role-based monitor all** command to enable the global monitor mode. If the **cts role-based monitor all** command is configured, the output of the **show cts role-based permissions** command displays monitor mode for all configured policies as true.

The following examples shows how to configure SGACL monitor from a source tag to a destination tag:

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

Related Commands

Command	Description
show cts role-based permissions	Displays the SGACL permission list.

cts role-based permissions

To enable permissions from a source group to a destination group, use the **cts role-based permissions** command in global configuration mode. To remove the permissions, use the **no** form of this command.

cts role-based permissions {**default** | **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

default	Specifies the default permissions list. Every cell (an SGT pair) for which, security group access control list (SGACL) permission is not configured statically or dynamically falls under the default category.
from	Specifies the source group tag of the filtered traffic.
sgt	Security Group Tag (SGT). Valid values are from 2 to 65519.
unknown	Specifies an unknown source or destination group tag.
rbacl-name	Role-based access control list (RBACL) or SGACL name. Up to 16 SGACLs can be specified in the configuration.
ipv4	Specifies the IPv4 protocol.
ipv6	Specifies the IPv6 protocol.

Command Default

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

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Use the **cts role-based permissions** command to define, replace, or delete the list of SGACLs for a given source group tag (SGT), destination group tag (DGT) pair. This policy is in effect as long as there is no dynamic policy for the same DGT or SGT.

The **cts role-based permissions default** command defines, replaces, or deletes the list of SGACLs of the default policy as long as there is no dynamic policy for the same DGT.

The following example shows how to enable permissions for a destination group:

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

Related Commands

Command	Description
show cts role-based permissions	Displays the SGACL permission list.

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.

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

Syntax Description

vlan-list *vlan-id*	(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.
all	(Optional) Selects all VLANs.

Command Default

SGT caching is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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.

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

Syntax Description

ipv4_netaddress | **ipv6_netaddress**	Specifies the network to be associated with an SGT. Enter IPv4 address in dot decimal notation; IPv6 in colon hexadecimal notation.
ipv4_netaddress/prefix | **ipv6_netaddress/prefix**	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
host {*ipv4_hostaddress* | *ipv6_hostaddress*}	Binds the specified host IP address with the SGT. Enter the IPv4 address in dot decimal notation; IPv6 in colon hexadecimal notation.
vlan-list {*vlan_ids* | **all**}	Specifies VLAN IDs. • (Optional) *vlan_ids*: Individual VLAN IDs are separated by commas, a range of IDs specified with a hyphen. • (Optional) **all**: Specifies all VLAN IDs.
vrf *instance_name*	Specifies a VRF instance, previously created on the device.
sgt *sgt-number*	Specifies the SGT number from 0 to 65,535.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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

Command	Description
show cts role-based sgt-map	Displays role-based access control information.

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*]}]
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

ipv4-address	SXP peer IPv4 address.
source	Specifies the source IPv4 address.
password	Specifies that an SXP password is used for the peer connection.
default	Specifies that the default SXP password is used.
none	Specifies no password is used.
mode	Specifies either the local or peer SXP connection mode.
local	Specifies that the SXP connection mode refers to the local device.
peer	Specifies that the SXP connection mode refers to the peer device.
listener	(Optional) Specifies that the device is the listener in the connection.
speaker	(Optional) Specifies that the device is the speaker in the connection.
hold-time *minimum-time maximum-time*	(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. **Note** If both minimum and maximum times are required, the *maximum-time* value must be greater than or equal to the *minimum-time* value.
vrf *vrf-name*	(Optional) Specifies the virtual routing and forwarding (VRF) instance name to the peer.
both	(Optional) Specifies that the device is both the speaker and the listener in the bidirectional SXP connection.

Command Default

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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
```

Related Commands

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

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.

cts sxp default password {**0** *unencrypted-pwd* | **6** *encrypted-key* | **7** *encrypted-keycleartext-pwd*}
no cts sxp default password {**0** *unencrypted-pwd* | **6** *encrypted-key* | **7** *encrypted-keycleartext-pwd*}

Syntax Description

0 *unencrypted-pwd*	Specifies that an unencrypted CTS-SXP default password follows. The maximum password length is 32 characters.
6 *encrypted-key*	Specifies that a 6 encryption type password is used as the CTS-SXP default password. The maximum password length is 32 characters.
7 *encrypted-key*	Specifies that a 7 encryption type password is used as the CTS-SXP default password. The maximum password length is 32 characters.
cleartext-pwd	Specifies a cleartext CTS-SXP default password. The maximum password length is 32 characters.

Command Default

Type **0** (cleartext)

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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
```

```
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

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

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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

Command	Description
cts sxp connectionpeer	Enters the CTS-SXP peer IP address and specifies if a password is used for the peer connection.
cts sxp default password	Configures the CTS-SXP default password.
cts sxp enable	Enables CTS-SXP on a device.
cts sxp log	Enables logging for IP-to-SGT binding changes.
cts sxp reconciliation	Changes the CTS-SXP reconciliation period.
cts sxp retry	Changes the CTS-SXP retry period timer.
show cts sxp	Displays the status of all SXP configurations.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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

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

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*}

Syntax Description

listener	Creates a filter group for a set of listeners.
speaker	Creates a filter group for a set of speakers.
global	Groups all speakers or listeners on the device.
filter-group-name	Name of the filter group.
filter-list-name	Name of the filter list.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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 a 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 precendence 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
```

Related Commands

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

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*

Syntax Description

filter-list-name	Name of the filter-list.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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 a 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, seperate 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
```

Related Commands

Command	Description
cts sxp filter-enable	Enable SXP IP-prefix and SGT-based filtering.
cts sxp filter-group	Creates a filter group for grouping a set of peers and applying a filter list to them.
show cts sxp filter-group	Displays information about the configured filter groups.
show cts sxp filter-list	Displays information about the configured filter lists.
debug cts sxp filter events	Logs events related to the creation, deletion and update of filter-lists and filter-groups.

cts sxp log binding-changes

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The **cts sxp log binding-changes** command enables logging for IP-to-SGT binding changes. SXP syslogs (sev 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

Command	Description
cts sxp connectionpeer	Enters the CTS-SXP peer IP address and specifies if a password is used for the peer connection
cts sxp default password	Configures the CTS-SXP default password.
cts sxp default source-ip	Configures the CTS-SXP source IPv4 address.
cts sxp enable	Enables CTS-SXP on a device.
cts sxp reconciliation	Changes the CTS-SXP reconciliation period.
cts sxp retry	Changes the CTS-SXP retry period timer.
show cts sxp	Displays status of all SXP configurations.

cts sxp reconciliation period

To change the Cisco TrustSec Security Group Tag (SGT) Exchange Protocol (CTS-SXP) reconciliation period, use the **cts sxp 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 sxp reconciliation period *seconds*
no cts sxp 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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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

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

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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

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

propagate sgt (cts manual)

To enable Security Group Tag (SGT) propagation at Layer 2 on Cisco TrustSec Security (CTS) interfaces, use the **propagate sgt** command in interface configuration mode. To disable SGT propagation, use the **no** form of this command.

propagate sgt

Syntax Description

This command has no arguments or keywords.

Command Default

SGT processing propagation is enabled.

Command Modes

CTS manual interface configuration mode (config-if-cts-manual)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

SGT processing propagation allows a CTS-capable interface to accept and transmit a CTS Meta Data (CMD) based L2 SGT tag. The **no propagate sgt** command can be used to disable SGT propagation on an interface in situations where a peer device is not capable of receiving an SGT, and as a result, the SGT tag cannot be put in the L2 header.

Examples

The following example shows how to disable SGT propagation on a manually-configured TrustSec-capable interface:

```
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

Command	Description
cts manual	Enables an interface for CTS.

Command	Description
show cts interface	Displays Cisco TrustSec states and statistics per interface.

sap mode-list (cts manual)

To select the Security Association Protocol (SAP) authentication and encryption modes (prioritized from highest to lowest) used to negotiate link encryption between two interfaces, use the **sap mode-list** command in CTS dot1x interface configuration mode. To remove a mode-list and revert to the default, use the **no** form of this command.

Use the **sap mode-list** command to manually specify the Pairwise Master Key (PMK) and the Security Association Protocol (SAP) authentication and encryption modes to negotiate MACsec link encryption between two interfaces. Use the **no** form of the command to disable the configuration.

sap pmk mode-list {**gcm-encrypt** | **gmac** | **no-encap** | **null**} [**gcm-encrypt** | **gmac** | **no-encap** | **null**]
no sap pmk mode-list {**gcm-encrypt** | **gmac** | **no-encap** | **null**} [**gcm-encrypt** | **gmac** | **no-encap** | **null**]

Syntax Description

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

Command Default

The default encryption is **sap pmk mode-list gcm-encrypt null**. When the peer interface does not support 802.1AE MACsec or 802.REV layer-2 link encryption, the default encryption is **null**.

Command Modes

CTS manual interface configuration (config-if-cts-manual)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Use the **sap pmk mode-list** command to specify the authentication and encryption method.

The Security Association Protocol (SAP) is an encryption key derivation and exchange protocol based on a draft version of the 802.11i IEEE protocol. SAP is used to establish and maintain the 802.1AE link-to-link encryption (MACsec) between interfaces that support MACsec.

SAP and the Pairwise Master Key (PMK) can be manually configured between two interfaces with the **sap pmk mode-list** command. When using 802.1X authentication, both sides (supplicant and authenticator) receive the PMK and the MAC address of the peer's port from the Cisco Secure Access Control Server.

If a device is running CTS-aware software but the hardware is not CTS-capable, disallow encapsulation with the **sap mode-list no-encap** command.

Examples

The following example shows how to configure SAP on a Gigabit Ethernet interface:

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

Related Commands

Command	Description
cts manual	Enables an interface for CTS.
propagate sgt (cts manual)	Enables Security Group Tag (SGT) propagation at Layer 2 on Cisco TrustSec Security (CTS) interfaces.
show cts interface	Displays Cisco TrustSec interface configuration statistics.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Examples

The following example displays output:

```
Device# show cts credentials

CTS password is defined in keystore, device-id = r4
```

Related Commands

Command	Description
cts credentials	Specifies the TrustSec ID and password.

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

port	(Optional) Gigabit Ethernet interface number. A verbose status output for this interface is returned.
number	(Optional) VLAN interface number from 1 to 4095.
brief	(Optional) Displays abbreviated status for all CTS interfaces.
summary	(Optional) Displays a tabular summary of all CTS interfaces with 4 or 5 key status fields for each interface.

Command Default

None

Command Modes

EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Use the **show cts interface** command without keywords to display verbose status for all CTS interfaces.

Examples

The following example displays output without using a keyword (verbose status for all CTS interfaces):

```
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:
```

```
    Propagate SGT:          Enabled
    Cache Info:
        Cache applied to link : NONE

    Statistics:
        authc success:              0
        authc reject:               0
        authc failure:              0
        authc no response:          0
        authc logoff:               0
        sap success:                0
        sap fail:                   0
        authz success:              0
        authz fail:                 0
        port auth fail:             0
        Ingress:
            control frame bypassed: 0
            sap frame bypassed:     0
            esp packets:            0
            unknown sa:             0
            invalid sa:             0
            inverse binding failed: 0
            auth failed:            0
            replay error:           0
        Egress:
            control frame bypassed: 0
            esp packets:            0
            sgt filtered:           0
            sap frame bypassed:     0
            unknown sa dropped:     0
            unknown sa bypassed:    0
```

The following example displays output using the **brief** keyword:

```
Device# show cts interface brief

Global Dot1x feature is Disabled
 Interface GigabitEthernet0/1/0:
     CTS is enabled, mode:    MANUAL
     IFC state:               OPEN
     Interface Active for 00:00:40.386
     Authentication Status:   NOT APPLICABLE
         Peer identity:       "unknown"
         Peer's advertised capabilities: ""
     Authorization Status:    NOT APPLICABLE
     SAP Status:              NOT APPLICABLE
     Propagate SGT:           Enabled
     Cache Info:
         Cache applied to link : NONE
```

Related Commands

Command	Description
cts manual	Enables an interface for CTS.
cts sxp enable	Configures SXP on a network device.
propagate sgt	Enables Security Group Tag (SGT) propagation at Layer 2 on Cisco TrustSec Security (CTS) interfaces.

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 [{**default** [{**ipv4** | **ipv6**}]}] [{**from** {*sgt-number* | **unknown**}[{**ipv4** | **ipv6** | **to** | {*sgt-number* | **unknown**} |[{**ipv4** | **ipv6**}]}]}][{**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

Field	Description
From	Source security group.
To	Destination security group.
SW-Permitt	Permitted traffic counters.
SW-Monitor	Denied traffic counters.

Related Commands

Command	Description
clear role-basedcounters	Resets SGACL statistic counters.
cts role-based	Maps IP addresses, Layer 3 interfaces, and VRFs to SGTs. Enables Cisco TrustSec caching and SGACL enforcement.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

This command displays the content of the SGACL permission matrix. You can specify the source security group tag (SGT) by using the **from** keyword and the destination SGT by using the **to** keyword. When both these keywords are specified RBACLs of a single cell are displayed. An entire column is displayed when only the **to** keyword is used. An entire row is displayed when the **from** keyword is used. The entire permission matrix is displayed when both the **from** and **to** keywords are omitted.

The command output is sorted by destination SGT as a primary key and the source SGT as a secondary key. SGACLs for each cell is displayed in the same order they are defined in the configuration or acquired from Cisco Identity Services Engine (ISE).

The **details** keyword is provided when a single cell is selected by specifying both **from** and **to** keywords. When the **details** keyword is specified the access control entries of SGACLs of a single cell are displayed.

The following is sample output from the **show role-based permissions** command:

```
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

Command	Description
cts role-based permissions	Enables permissions from a source group to a destination group.
cts role-based monitor	Enables role-based access list monitoring.

show cts server-list

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

show cts server-list

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.
Cisco IOS XE Amsterdam 17.1.1	The output of this command was modified to display the HTTP server address and status information.
Cisco IOS XE Amsterdam 17.2.1	The output of this command was modified to display the IPv6 address of the HTTP servers.

Usage Guidelines

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

In Cisco IOS XE Gibraltar 17.1.1 and later releases, the output of this command displays HTTP server address and their status information.

In Cisco IOS XE Gibraltar 17.2.1 and later releases, the output of this command displays the IPv6 address along with the IPv4 address of HTTP servers.

Examples

Cisco IOS XE Amsterdam 17.2.1 and later releases

The following sample output from the **show cts server-list** command displays IPv4 and IPv6 address of HTTP servers and their status information:

```
Device> show cts server-list

HTTP Server-list:
  Server Name  : cts_private_server_0
  Server State : ALIVE
  IPv4 Address     : 10.64.69.151
  IPv6 Address     : 2001:DB8:8086:6502::
  IPv6 Address     : 2001:db8::2
  IPv6 Address     : 2001:db8::402:99
  IPv6 Address     : 2001:DB8::802:16
  Domain-name      : ise-267.cisco.com
  Trustpoint       : cts_trustpoint_0

  Server Name  : cts_private_server_1
  Server State : ALIVE
  IPv4 Address     : 10.10.10.3
  IPv4 Address     : 10.10.10.2
  IPv6 Address     : 2001:db8::20
  IPv6 Address     : 2001:db8::21
```

```
  Domain-name      : www.ise.cisco.com
  Trustpoint       : cts_trustpoint_1
```

Cisco IOS XE Amsterdam 17.1.1

The following sample output from the **show cts server-list** command displays HTTP servers and their status information:

```
Device> show cts server-list

HTTP Server-list:
Server Name: Http_Server_1
Server Status: DEAD
    IPv4 Address: 10.78.105.148
    IPv6 Address: Not Supported
    Domain-name: http_server_1.ise.com
    Port: 9063


Server Name: Http_Server_2
Server Status: ALIVE
    IPv4 Address: 10.78.105.149
    IPv6 Address: Not Supported
    Domain-name: http_server_2.ise.com
    Status = ALIVE
```

Prior to Cisco IOS XE Amsterdam 17.1.1

The following example displays the Cisco TrustSec 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

Command	Description
address ipv4 (config-radius-server)	Configures the RADIUS server accounting and authentication parameters for PAC provisioning.
pac key	Specifies the PAC encryption key.

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

connections	Displays Cisco TrustSec SXP connections information.
brief	(Optional) Displays an abbreviation of the SXP information.
vrf *instance-name*	(Optional) Displays the SXP information for the specified Virtual Routing and Forwarding (VRF) instance name.
filter-group {**detailed | global | listener | speaker** }	(Optional) Displays filter group information.
filter-list *filter-list-name*	(Optional) Displays filter list information.
sgt-map	(Optional) Displays the IP-to-SGT mappings received through SXP.

Command Default

None

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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
```

```
 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

Command	Description
cts sxp connection peer	Enters the Cisco TrustSec SXP peer IP address and specifies if a password is used for the peer connection
cts sxp default password	Configures the Cisco TrustSec SXP default password.
cts sxp default source-ip	Configures the Cisco TrustSec SXP source IPv4 address.
cts sxp enable	Enables Cisco TrustSec SXP on a device.
cts sxp log	Enables logging for IP-to-SGT binding changes.
cts sxp reconciliation	Changes the Cisco TrustSec SXP reconciliation period.
cts sxp retry	Changes the Cisco TrustSec SXP retry period timer.

show platform hardware fed switch active fwd-asic resource tcam utilization

To display CAM utilization information for ASIC, use the **show platform hardware fed switch active fwd-asic resource tcam utilization** command in privileged EXEC mode.

show platform hardware fed switch active fwd-asic resource tcam utilization [*asic-number*] [*slice-id*]

Syntax Description

asic-number	Displays the ASIC number. Valid values are from 0 to 7.
slice-id	Displays per slice usage.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following is sample output from the **show platform hardware fed switch active fwd-asic resource tcam utilization** command:

```
Device# enable
Device# show platform hardware fed switch active fwd-asic resource tcam utilization

CAM Utilization for ASIC  [0]
 Table                  Subtype      Dir      Max     Used    %Used       V4       V6
MPLS    Other

----------------------------------------------------------------------------------------------

 Mac Address Table      EM           I       32768       25    0.08%        0        0
    0       25
 Mac Address Table      TCAM         I        1024       22    2.15%        0        0
    0       22
 L3 Multicast           EM           I        8192        0    0.00%        0        0
    0        0
 L3 Multicast           TCAM         I         512        9    1.76%        3        6
    0        0
 L2 Multicast           EM           I        8192        0    0.00%        0        0
    0        0
 L2 Multicast           TCAM         I         512       11    2.15%        3        8
    0        0
 IP Route Table         EM           I       24576       14    0.06%       13        0
    1        0
 IP Route Table         TCAM         I        8192       30    0.37%       11       16
    2        1
 QOS ACL                TCAM         IO       5120       85    1.66%       28       38
    0       19
                        TCAM         I                   45    0.88%       15       20
    0       10
                        TCAM         O                   40    0.78%       13       18
    0        9
```

```
Security ACL           TCAM         IO       5120      131    2.56%       26       60
   0       45
                       TCAM         I                  88    1.72%       12       36
   0       40
                       TCAM         O                  43    0.84%       14       24
   0        5
Netflow ACL            TCAM         I         256        6    2.34%        2        2
   0        2
PBR ACL                TCAM         I        1024       36    3.52%       30        6
   0        0
Netflow ACL            TCAM         O         768        6    0.78%        2        2
   0        2
Flow SPAN ACL          TCAM         IO       1024       13    1.27%        3        6
   0        4
                       TCAM         I                   5    0.49%        1        2
   0        2
                       TCAM         O                   8    0.78%        2        4
   0        2
Control Plane          TCAM         I         512      290   56.64%      138      106
   0       46
Tunnel Termination     TCAM         I         512       22    4.30%        9       13
   0        0
Lisp Inst Mapping      TCAM         I        2048        2    0.10%        0        0
   0        2
Security Association   TCAM         I         256        4    1.56%        2        2
   0        0
CTS Cell Matrix/VPN
Label                  EM           O        8192        0    0.00%        0        0
   0        0
CTS Cell Matrix/VPN
Label                  TCAM         O         512        1    0.20%        0        0
   0        1
Client Table           EM           I        4096        0    0.00%        0        0
   0        0
Client Table           TCAM         I         256        0    0.00%        0        0
   0        0
Input Group LE         TCAM         I        1024        0    0.00%        0        0
   0        0
Output Group LE        TCAM         O        1024        0    0.00%        0        0
   0        0
Macsec SPD             TCAM         I         256        2    0.78%        0        0
   0        2
```

Output fields are self-explanatory.

Related Commands

Command	Description
show platform hardware fed switch active fwd-asic resource tcam table	Displays the current CAM table.
show platform hardware fed switch active fwd-asic resource tcam usage	Displays the current CAM usage.

show platform hardware fed switch active sgacl resource usage

To display Security Group access control list (SGACL) resource information for Application Specific Integrated Circuit (ASIC), use the **show platform hardware fed switch active sgacl resource usage** command in privileged EXEC mode.

show platform hardware fed switch active sgacl resource usage

Syntax Description

usage	Displays SGACL resource usage.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following is a sample output from the **show platform hardware fed switch active sgacl resource usage** command:

```
Device# enable
Device# show platform hardware fed switch active sgacl resource usage

SGACL RESOURCE DETAILS ASIC :#0
================================
                                                    Percent     Thresholds
Hardware Resource               MAX      Used       Used    Upper     Lower
-------------------------------------------------------------------------------
  CTS Cell Matrix Config    :                                  80        70
  CTS Cell Matrix Entries   :   8192         0         0         Normal
  CTS Cell Overflow Entries :    512         1         0

  Policy Configuration      :                                  80        70
  Policy Entries            :    256         3         1         Normal

  DGT Config                :                                  80        70
  DGT Entries               :   4096         0         0         Normal

  Security ACL Configured   :                                  80        70
  Security ACL Entries      :   5120       131         2         Normal

                                Total     Percent
      SGACL TCAM Entries         Used      Used
      ------------------------------------------------------------------
      Output PRE SGACL      :        4        12
      Output SGACL          :        0         0
      Output SGACL DEFAULT  :        0         0
.
.
.
Device#
```

Output fields are self-explanatory.

show platform software classification switch active F0 class-group-manager class-group client acl all

To display ACL class group ID, which is used to view Ternary Content Addressable Memory(TCAM) entry, use the **show platform software classification switch active F0 class-group-manager class-group client acl all** command in privileged EXEC mode.

show platform software classification switch active F0 class-group-manager class-group client acl all

Syntax Description

class-group-manager	Displays the class group manager.
class-group	Displays the class group.
all	Displays the ACL class group ID for all class groups.

Command Modes

Privileged EXEC (#)

Command History

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

Example

The following is a sample output from the **show platform software classification switch active F0 class-group-manager class-group client acl all** command:

```
Device#show platform software classification switch active F0 class-group-manager class-group
 client acl all

QFP classification class client all group

  class-group [ACL-GRP:273]
  class-group [ACL-GRP:529]
  class-group [ACL-GRP:801]
```

Output fields are self-explanatory.

Related Commands

Command	Description
show platform software classification switch active F0 class-group-manager class-group client acl name *class-group name*	Displays ACL class group information for the specified class group.
show platform software classification switch active F0 class-group-manager class-group client acl *class-group id*	Displays ACL class group information for the specified class group.

show platform software cts forwarding-manager switch active F0 port

To display CTS information for forwarding manager interfaces, use the **show platform software cts forwarding-manager switch active F0 port** command in privileged EXEC mode.

show platform software cts forwarding-manager switch active F0 port

Syntax Description

F0	Embedded service processor slot 0.
port	Displays the port CTS status.

Command Modes

Privileged EXEC (#)

Command History

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

Example

The following is a sample output from the **show platform software cts forwarding-manager switch active F0 port** command:

```
Device#show platform software cts forwarding-manager switch active F0 port

Forwarding Manager Interfaces CTS Information

Name                              ID     CTS Enable  Trusted   Propagate   SGT value
-------------------------------------------------------------------------------------
GigabitEthernet1/0/1              77         0          0          0           0
GigabitEthernet1/0/3              79         0          0          0           0
GigabitEthernet1/0/4              80         0          0          0           0
GigabitEthernet1/0/5              81         0          0          0           0
GigabitEthernet1/0/6              82         0          0          0           0
GigabitEthernet1/0/7              83         0          0          0           0
GigabitEthernet1/0/8              84         0          0          0           0
GigabitEthernet1/0/9              85         0          0          0           0
GigabitEthernet1/0/10             86         0          0          0           0
GigabitEthernet1/0/11             87         0          0          0           0
GigabitEthernet1/0/12             88         0          0          0           0
GigabitEthernet1/0/13             89         0          0          0           0
GigabitEthernet1/0/14             90         0          0          0           0
GigabitEthernet1/0/15             91         0          0          0           0
GigabitEthernet1/0/16             92         0          0          0           0
GigabitEthernet1/0/17             93         0          0          0           0
GigabitEthernet1/0/18             94         0          0          0           0
GigabitEthernet1/0/19             95         0          0          0           0
GigabitEthernet1/0/20             96         0          0          0           0
GigabitEthernet1/0/21             97         0          0          0           0
GigabitEthernet1/0/22             98         0          0          0           0
GigabitEthernet1/0/23             99         0          0          0           0
GigabitEthernet1/0/24            100         0          0          0           0
GigabitEthernet1/0/25            101         0          0          0           0
GigabitEthernet1/0/26            102         0          0          0           0
```

```
GigabitEthernet1/0/27          103         0          0          0          0
GigabitEthernet1/0/28          104         0          0          0          0
GigabitEthernet1/0/29          105         0          0          0          0
GigabitEthernet1/0/30          106         0          0          0          0
GigabitEthernet1/0/31          107         0          0          0          0
GigabitEthernet1/0/32          108         0          0          0          0
GigabitEthernet1/0/33          109         0          0          0          0
GigabitEthernet1/0/34          110         0          0          0          0
GigabitEthernet1/0/35          111         0          0          0          0
GigabitEthernet1/0/36          112         0          0          0          0
GigabitEthernet1/0/37          113         0          0          0          0
GigabitEthernet1/0/38          114         0          0          0          0
GigabitEthernet1/0/39          115         0          0          0          0
GigabitEthernet1/0/40          116         0          0          0          0
GigabitEthernet1/0/41          117         0          0          0          0


Forwarding Manager Interfaces CTS Information

Name                            ID     CTS Enable  Trusted   Propagate   SGT value
-------------------------------------------------------------------------------------
GigabitEthernet1/0/42          118         0          0          0          0
GigabitEthernet1/0/43          119         0          0          0          0
GigabitEthernet1/0/44          120         0          0          0          0
GigabitEthernet1/0/45          121         0          0          0          0
GigabitEthernet1/0/46          122         0          0          0          0
GigabitEthernet1/0/47          123         0          0          0          0
GigabitEthernet1/1/1           125         0          0          0          0
GigabitEthernet1/1/2           126         0          0          0          0
GigabitEthernet1/1/3           127         0          0          0          0
GigabitEthernet1/1/4           128         0          0          0          0
TenGigabitEthernet1/1/1        129         0          0          0          0
TenGigabitEthernet1/1/2        130         0          0          0          0
TenGigabitEthernet1/1/3        131         0          0          0          0
TenGigabitEthernet1/1/4        132         0          0          0          0
TenGigabitEthernet1/1/5        133         0          0          0          0
TenGigabitEthernet1/1/6        134         0          0          0          0
TenGigabitEthernet1/1/7        135         0          0          0          0
TenGigabitEthernet1/1/8        136         0          0          0          0
FortyGigabitEthernet1/1/1      137         0          0          0          0
FortyGigabitEthernet1/1/2      138         0          0          0          0
TwentyFiveGigE1/1/1            139         0          0          0          0
TwentyFiveGigE1/1/2            140         0          0          0          0
AppGigabitEthernet1/0/1        141         0          0          0          0
GigabitEthernet2/0/1           142         1          0          0          0
GigabitEthernet2/0/2           143         0          0          0          0
GigabitEthernet2/0/3           144         0          0          0          0
GigabitEthernet2/0/4           145         0          0          0          0
GigabitEthernet2/0/5           146         0          0          0          0
GigabitEthernet2/0/6           147         0          0          0          0
GigabitEthernet2/0/7           148         0          0          0          0
GigabitEthernet2/0/8           149         0          0          0          0
GigabitEthernet2/0/9           150         0          0          0          0
GigabitEthernet2/0/10          151         0          0          0          0
GigabitEthernet2/0/11          152         0          0          0          0
GigabitEthernet2/0/12          153         0          0          0          0
GigabitEthernet2/0/13          154         0          0          0          0
GigabitEthernet2/0/14          155         0          0          0          0
GigabitEthernet2/0/15          156         0          0          0          0
GigabitEthernet2/0/16          157         0          0          0          0
GigabitEthernet2/0/17          158         0          0          0          0


Forwarding Manager Interfaces CTS Information
```

```
Name                              ID     CTS Enable  Trusted   Propagate   SGT value
-------------------------------------------------------------------------------------
GigabitEthernet2/0/18            159          0          0          0           0
GigabitEthernet2/0/19            160          0          0          0           0
GigabitEthernet2/0/20            161          0          0          0           0
GigabitEthernet2/0/21            162          0          0          0           0
GigabitEthernet2/0/22            163          0          0          0           0
GigabitEthernet2/0/23            164          0          0          0           0
GigabitEthernet2/0/24            165          0          0          0           0
GigabitEthernet2/0/25            166          0          0          0           0
GigabitEthernet2/0/26            167          0          0          0           0
GigabitEthernet2/0/27            168          0          0          0           0
GigabitEthernet2/0/28            169          0          0          0           0
GigabitEthernet2/0/29            170          0          0          0           0
GigabitEthernet2/0/30            171          0          0          0           0
GigabitEthernet2/0/31            172          0          0          0           0
GigabitEthernet2/0/32            173          0          0          0           0
GigabitEthernet2/0/33            174          0          0          0           0
GigabitEthernet2/0/34            175          0          0          0           0
GigabitEthernet2/0/35            176          0          0          0           0
GigabitEthernet2/0/36            177          0          0          0           0
GigabitEthernet2/0/37            178          0          0          0           0
GigabitEthernet2/0/38            179          0          0          0           0
GigabitEthernet2/0/39            180          0          0          0           0
GigabitEthernet2/0/40            181          0          0          0           0
GigabitEthernet2/0/41            182          0          0          0           0
GigabitEthernet2/0/42            183          0          0          0           0
GigabitEthernet2/0/43            184          0          0          0           0
GigabitEthernet2/0/44            185          0          0          0           0
GigabitEthernet2/0/45            186          0          0          0           0
GigabitEthernet2/0/46            187          0          0          0           0
GigabitEthernet2/0/47            188          0          0          0           0
GigabitEthernet2/1/1             190          0          0          0           0
GigabitEthernet2/1/2             191          0          0          0           0
GigabitEthernet2/1/3             192          0          0          0           0
GigabitEthernet2/1/4             193          0          0          0           0
TenGigabitEthernet2/1/1          194          0          0          0           0
TenGigabitEthernet2/1/2          195          0          0          0           0
TenGigabitEthernet2/1/3          196          0          0          0           0
TenGigabitEthernet2/1/4          197          0          0          0           0
TenGigabitEthernet2/1/5          198          0          0          0           0
TenGigabitEthernet2/1/6          199          0          0          0           0


Forwarding Manager Interfaces CTS Information

Name                              ID     CTS Enable  Trusted   Propagate   SGT value
-------------------------------------------------------------------------------------
TenGigabitEthernet2/1/7          200          0          0          0           0
TenGigabitEthernet2/1/8          201          0          0          0           0
FortyGigabitEthernet2/1/1        202          0          0          0           0
FortyGigabitEthernet2/1/2        203          0          0          0           0
TwentyFiveGigE2/1/1              204          0          0          0           0
TwentyFiveGigE2/1/2              205          0          0          0           0
AppGigabitEthernet2/0/1          206          0          0          0           0
GigabitEthernet1/0/2             213          0          0          0           0
```

The following table explains the significant fields shown in the output:

Table 7: show platform software cts forwarding-manager switch active F0 port Field Descriptions

Field	Description

Name	The name of the interface.
ID	The interface ID.
CTS Enable	The status of CTS.
Trusted	The trusted status of the interface.
Propagate	The propagation status of the interface.
SGT value	The value of SGT.

show platform software cts forwarding-manager switch active F0

To display Security Group Tag (SGT) binding table, use the **show platform software cts forwarding-manager switch active F0** command in privileged EXEC mode.

show platform software cts forwarding-manager switch active F0

Syntax Description

F0	Selects embedded service processor slot 0.

Command Modes

Privileged EXEC (#)

Command History

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

Example

The following is a sample output from the **show platform software cts forwarding-manager switch active F0** command:

```
Device#show platform software cts forwarding-manager switch active F0

SGT Binding Table

Number of bindings: 1

2.2.2.2/32
SGT Src: 2
SGT Dst: 2


SGT Binding Table
```

Output fields are self-explanatory.

Related Commands

Command	Description
show platform software cts forwarding-manager switch active F0 port	Displays the port CTS status.
show platform software cts forwarding-manager switch active F0 permissions	Displays the SGACL permissions.

show platform software cts forwarding-manager switch active F0 permissions

To display Security group access control lists (SGACLs) permissions, use the **show platform software cts forwarding-manager switch active F0 permissions** command in privileged EXEC mode.

show platform software cts forwarding-manager switch active F0 permissions

Syntax Description

F0	Selects embedded service processor slot 0.
permissions	Displays SGACL permissions.

Command Modes

Privileged EXEC (#)

Command History

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

Example

The following is sample output from the **show platform software cts forwarding-manager switch active F0 permissions** command:

```
Device#show platform software cts forwarding-manager switch active F0 permissions

Forwarding Manager CTS permissions Information

  sgt       dgt     ACL Group Name


   4         2      V4SGACL7100

 65535     65535    V4SGACL8100

 65535     65535    V6SGACL9100
```

The following table explains the significant fields shown in the output:

Table 8: show platform software cts forwarding-manager switch active F0 permissions Field Descriptions

Field	Description
sgt	The source group tag.
dgt	The destination group tag.

ACL Group Name	The name of the ACL group.

show platform software fed switch active acl counters hardware | inc SGACL

To display counters from the forwarding engine driver, use the **show platform software fed switch active acl counters hardware | inc SGACL** command in privileged EXEC mode.

show platform software fed switch active acl counters hardware | inc SGACL

Syntax Description

counters	Displays counter information.
hardware	Displays hardware counters.
include	Includes lines that match the specified string.

Command Modes

Privileged EXEC (#)

Command History

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

Example

The following is a sample output from the **show platform software fed switch active acl counters hardware | inc SGACL** command:

```
Device# show platform software fed switch active acl counters hardware | inc SGACL

Egress IPv4 SGACL Drop           (0x3f000061):          0 frames
Egress IPv6 SGACL Drop           (0x13000062):          0 frames
Egress IPv4 SGACL Test Cell Drop (0xd2000063):          0 frames
Egress IPv6 SGACL Test Cell Drop (0x40000064):          0 frames
Egress IPv4 Pre SGACL Forward    (0x2c000067):          0 frames
```

show platform software fed switch active acl usage

To display Security Group access control lists (SGACLs) usage, use the **show platform software fed switch active acl usage** command in privileged EXEC mode.

show platform software fed switch active acl usage

Syntax Description

usage	Displays ACL usage.

Command Modes

Privileged EXEC (#)

Command History

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

Example

The following is sample output from the **show platform software fed switch active acl usage** command:

```
Device# show platform software fed switch active acl usage
##########################################################
########                                  ##################
#######      Printing Usage Infos         ##################
########                                  ##################
##########################################################
#####  ACE Software VMR max:196608 used:282
##########################################################
=============================================================================================================
Feature Type            ACL Type        Dir             Name                    Entries
Used
SGACL                   IPV4            Egress          V4SGACL7100             2

=============================================================================================================
Feature Type            ACL Type        Dir             Name                    Entries
Used
SGACL_CATCHALL          IPV4            Egress          V4SGACL8100             1

=============================================================================================================
Feature Type            ACL Type        Dir             Name                    Entries
Used
SGACL_CATCHALL          IPV6            Egress          V6SGACL9100             1

=============================================================================================================
```

Output fields are self-explanatory.

show platform software fed switch active ifm mappings

show platform software fed switch active ifm mappings

Syntax Description

ifm	Displays interface manager information.
mappings	Displays interface to hardware mapping information.

Command Modes

Privileged EXEC (#)

Command History

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

Example

The following is a sample output from the **show platform software fed switch active ifm mappings** command:

```
Device#show platform software fed switch active ifm mappings

Interface               IF_ID    Inst Asic Core Port SubPort Mac  Cntx LPN  GPN  Type
Active
GigabitEthernet3/0/1    0xa        1   0   1    0      0      26   6    1    193  NIF  Y
GigabitEthernet3/0/2    0xb        1   0   1    1      0      6    7    2    194  NIF  Y
GigabitEthernet3/0/3    0xc        1   0   1    2      0      28   8    3    195  NIF  Y
GigabitEthernet3/0/4    0xd        1   0   1    3      0      27   9    4    196  NIF  Y
GigabitEthernet3/0/5    0xe        1   0   1    4      0      30   10   5    197  NIF  Y
GigabitEthernet3/0/6    0xf        1   0   1    5      0      29   11   6    198  NIF  Y
GigabitEthernet3/0/7    0x10       1   0   1    6      0      32   12   7    199  NIF  Y
GigabitEthernet3/0/8    0x11       1   0   1    7      0      31   13   8    200  NIF  Y
GigabitEthernet3/0/9    0x12       1   0   1    8      0      19   14   9    201  NIF  Y
GigabitEthernet3/0/10   0x13       1   0   1    9      0      5    15   10   202  NIF  Y
GigabitEthernet3/0/11   0x14       1   0   1    10     0      21   16   11   203  NIF  Y
GigabitEthernet3/0/12   0x15       1   0   1    11     0      20   17   12   204  NIF  Y
GigabitEthernet3/0/13   0x16       1   0   1    12     0      23   18   13   205  NIF  Y
GigabitEthernet3/0/14   0x17       1   0   1    13     0      22   19   14   206  NIF  Y
GigabitEthernet3/0/15   0x18       1   0   1    14     0      25   20   15   207  NIF  Y
GigabitEthernet3/0/16   0x19       1   0   1    15     0      24   21   16   208  NIF  Y
GigabitEthernet3/0/17   0x1a       1   0   1    16     0      12   22   17   209  NIF  Y
GigabitEthernet3/0/18   0x1b       1   0   1    17     0      4    23   18   210  NIF  Y
GigabitEthernet3/0/19   0x1c       1   0   1    18     0      14   24   19   211  NIF  Y
GigabitEthernet3/0/20   0x1d       1   0   1    19     0      13   25   20   212  NIF  Y
GigabitEthernet3/0/21   0x1e       1   0   1    20     0      16   26   21   213  NIF  Y
GigabitEthernet3/0/22   0x1f       1   0   1    21     0      15   27   22   214  NIF  Y
GigabitEthernet3/0/23   0x20       1   0   1    22     0      18   28   23   215  NIF  Y
GigabitEthernet3/0/24   0x21       1   0   1    23     0      17   29   24   216  NIF  Y
GigabitEthernet3/0/25   0x22       0   0   0    24     0      26   6    25   217  NIF  Y
GigabitEthernet3/0/26   0x23       0   0   0    25     0      6    7    26   218  NIF  Y
GigabitEthernet3/0/27   0x24       0   0   0    26     0      28   8    27   219  NIF  Y
GigabitEthernet3/0/28   0x25       0   0   0    27     0      27   9    28   220  NIF  Y
GigabitEthernet3/0/29   0x26       0   0   0    28     0      30   10   29   221  NIF  Y
GigabitEthernet3/0/30   0x27       0   0   0    29     0      29   11   30   222  NIF  Y
GigabitEthernet3/0/31   0x28       0   0   0    30     0      32   12   31   223  NIF  Y
GigabitEthernet3/0/32   0x29       0   0   0    31     0      31   13   32   224  NIF  Y
GigabitEthernet3/0/33   0x2a       0   0   0    32     0      19   14   33   225  NIF  Y
GigabitEthernet3/0/34   0x2b       0   0   0    33     0      5    15   34   226  NIF  Y
GigabitEthernet3/0/35   0x2c       0   0   0    34     0      21   16   35   227  NIF  Y
```

```
GigabitEthernet3/0/36      0x2d       0    0    0     35     0       20    17    36    228   NIF   Y
GigabitEthernet3/0/37      0x2e       0    0    0     36     0       23    18    37    229   NIF   Y
GigabitEthernet3/0/38      0x2f       0    0    0     37     0       22    19    38    230   NIF   Y
GigabitEthernet3/0/39      0x30       0    0    0     38     0       25    20    39    231   NIF   Y
GigabitEthernet3/0/40      0x31       0    0    0     39     0       24    21    40    232   NIF   Y
GigabitEthernet3/0/41      0x32       0    0    0     40     0       12    22    41    233   NIF   Y
GigabitEthernet3/0/42      0x33       0    0    0     41     0       4     23    42    234   NIF   Y
GigabitEthernet3/0/43      0x34       0    0    0     42     0       14    24    43    235   NIF   Y
GigabitEthernet3/0/44      0x35       0    0    0     43     0       13    25    44    236   NIF   Y
GigabitEthernet3/0/45      0x36       0    0    0     44     0       16    26    45    237   NIF   Y
GigabitEthernet3/0/46      0x37       0    0    0     45     0       15    27    46    238   NIF   Y
GigabitEthernet3/0/47      0x38       0    0    0     46     0       18    28    47    239   NIF   Y
GigabitEthernet3/0/48      0xd8       0    0    0     47     0       17    29    48    240   NIF   Y
GigabitEthernet3/1/1       0x3a       1    0    1     48     0       3     4     49    241   NIF   N
GigabitEthernet3/1/2       0x3b       1    0    1     49     0       2     5     50    242   NIF   N
GigabitEthernet3/1/3       0x3c       0    0    0     50     0       3     4     51    243   NIF   N
GigabitEthernet3/1/4       0x3d       0    0    0     51     0       2     5     52    244   NIF   N
TenGigabitEthernet3/1/1    0x3e       1    0    1     52     0       3     3     53    245   NIF   N
TenGigabitEthernet3/1/2    0x3f       1    0    1     53     0       2     2     54    246   NIF   N
TenGigabitEthernet3/1/3    0x40       1    0    1     54     0       1     1     55    247   NIF   N
TenGigabitEthernet3/1/4    0x41       1    0    1     55     0       0     0     56    248   NIF   N
TenGigabitEthernet3/1/5    0x42       0    0    0     56     0       3     3     57    249   NIF   N
TenGigabitEthernet3/1/6    0x43       0    0    0     57     0       2     2     58    250   NIF   N
TenGigabitEthernet3/1/7    0x44       0    0    0     58     0       1     1     59    251   NIF   N
TenGigabitEthernet3/1/8    0x45       0    0    0     59     0       0     0     60    252   NIF   N
FortyGigabitEthernet3/1/1  0x46       1    0    1     60     0       0     0     61    253   NIF   N
FortyGigabitEthernet3/1/2  0x47       0    0    0     61     0       0     0     62    254   NIF   N
TwentyFiveGigE3/1/1        0x48       1    0    1     62     0       0     0     63    255   NIF   N
TwentyFiveGigE3/1/2        0x49       0    0    0     63     0       0     0     64    256   NIF   N
AppGigabitEthernet3/0/1    0x4a       1    0    1     24     0       11    30    65    257   NIF   Y
```

The following table explains the significant fields shown in the output:

Table 9: show platform software fed switch active ifm mappings Field Descriptions

Field	Description
Interface	The name of the interface.
IF_ID	The interface ID.
Inst	The instance ID.
Asic	The ASIC number.
Core	The core number.
Port	The port number of the interface.
SubPort	The number of subports.
MAC	The MAC address.
LPN	The local port number inside ASIC.
GPN	The global system number inside switch.
Type	The type of interface.
Active	The interface status (active/inactive).

show platform software fed switch active ip route

To display IP route information, use the **show platform software fed switch active ip route** command in privileged EXEC mode.

show platform software fed switch active ip route

Syntax Description

ip	Accepts IP commands.
route	Displays IPv4 Forwarding Information Base (FIB) details.

Command Modes

Privileged EXEC (#)

Command History

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

Example

The following is sample output from the **show platform software fed switch active ip route** command:

```
Device# show platform software fed switch active ip route
vrf   dest                                      htm            flags   SGT   DGID MPLS
 Last-modified            SecsSinceHit
---   ----                                      ---            -----   ---   ---- ----
 ------------------------ ------------
2     0.0.0.0/0                                 0x78f2fd3488a8 0x0     0     0
 2023/03/14 06:38:18.684           1
2     127.0.0.0/8                               0x78f2fd351508 0x0     0     0
 2023/03/14 06:38:18.687           1
2     255.255.255.255/32                        0x78f2fd34ebd8 0x0     0     0
 2023/03/14 06:38:18.686           1
2     240.0.0.0/4                               0x78f2fd350828 0x0     0     0
 2023/03/14 06:38:18.686           1
2     0.0.0.0/32                                0x78f2fd34cd88 0x0     0     0
 2023/03/14 06:38:18.685           1
2     0.0.0.0/8                                 0x78f2fd350e98 0x0     0     0
 2023/03/14 06:38:18.686           1
0     0.0.0.0/0                                 0x78f2fd345388 0x0     0     0
 2023/03/14 06:39:09.383         352
0     9.24.0.0/32                               0x78f2fd33e1c8 0x0     0     0
 2023/03/14 06:38:38.930           1
0     9.24.0.1/32                               0x78f2fd33a5e8 0x0     0     0
 2023/03/14 06:39:09.390           5
0     127.0.0.0/8                               0x78f2fd3501b8 0x0     0     0
 2023/03/14 06:38:18.686           1
0     255.255.255.255/32                        0x78f2fd34c478 0x0     0     0
 2023/03/14 06:38:18.685           1
0     2.2.2.2/32                                0x78f2fd3568e8 0x0     2     1
 2023/03/14 06:39:09.383           1
0     9.24.255.255/32                           0x78f2fd344838 0x0     0     0
 2023/03/14 06:38:38.931           1
0     10.64.69.164/32                           0x78f2fd33fac8 0x0     0     0
 2023/03/14 06:39:09.383           1
0     10.77.128.69/32                           0x78f2fd3420a8 0x0     0     0
 2023/03/14 06:39:09.383           1
0     240.0.0.0/4                               0x78f2fd34f4d8 0x0     0     0
```

```
 2023/03/14 06:38:18.686            1
0     10.106.26.249/32                              0x78f2fd3399a8 0x0     0      0
 2023/03/14 06:39:09.383            1
0     0.0.0.0/32                                    0x78f2fd34a768 0x0     0      0
 2023/03/14 06:38:18.685            1
0     9.24.23.30/32                                 0x78f2fd1f2078 0x0     0      0
 2023/03/14 06:38:38.930           24
0     9.24.0.0/16                                   0x78f2fd33af48 0x0     0      0
 2023/03/14 06:38:38.930            1
0     0.0.0.0/8                                     0x78f2fd34fb48 0x0     0      0
 2023/03/14 06:38:18.686            1
```

The following table explains the significant fields shown in the output:

Table 10: show platform software fed switch active ip route Field Descriptions

Field	Description
vrf	The VRF ID.
dest	The destination address.
htm	The hash table manager object pointer for IP route.
SGT	The security group tag.
DGID	The destination tag ID.

show platform software fed switch active sgacl detail

To display global enforcement status along with policy and count information, use the **show platform software fed switch active sgacl detail** command in privileged EXEC mode.

show platform software fed switch active sgacl detail

Syntax Description

sgacl	Displays SGACL hardware information.
detail	Displays detailed SGACL information.

Command Modes

Privileged EXEC (#)

Command History

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

Example

The following is a sample output from the **show platform software fed switch active sgacl detail** command:

```
Device# show platform software fed switch active sgacl detail
Global Enforcement: Off

*Refcnt: for the non-SGACL feature
=================================== DGID Table ===================================
SGT/Refcnt          DGT        DGID         test_cell monitor   permitted      denied
==================================================================================
*/3                   2           1
```

The following table explains the significant fields shown in the output:

Table 11: show platform software fed switch active sgacl detail Field Descriptions

Field	Description
SGT/Refcnt	The security group tag/reinforcement.
DGT	The destination tag.
DGID	The destination tag ID.

show platform software fed switch active sgacl port

To display Layer 2 interface configuration settings for all interfaces, use the **show platform software fed switch active sgacl port** command in privileged EXEC mode.

show platform software fed switch active sgacl port

Syntax Description

sgacl	Displays Security Group access control lists (SGACLs) hardware information.
port	Specifies port configuration.

Command History

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

Example

The following is a sample output from the **show platform software fed switch active sgacl port** command:

```
Device# show platform software fed switch active sgacl port

Port            Status     Port-SGT  Trust  Propagate  IngressCache EgressCache
-------------------------------------------------------------------------------
Gi3/0/1        Disabled        0     No      No          No          No
Gi3/0/2        Disabled        0     No      No          No          No
Gi3/0/3        Disabled        0     No      No          No          No
Gi3/0/4        Disabled        0     No      No          No          No
Gi3/0/5        Disabled        0     No      No          No          No
Gi3/0/6        Disabled        0     No      No          No          No
Gi3/0/7        Disabled        0     No      No          No          No
Gi3/0/8        Disabled        0     No      No          No          No
Gi3/0/9        Disabled        0     No      No          No          No
Gi3/0/10       Disabled        0     No      No          No          No
Gi3/0/11       Disabled        0     No      No          No          No
Gi3/0/12       Disabled        0     No      No          No          No
Gi3/0/13       Disabled        0     No      No          No          No
Gi3/0/14       Disabled        0     No      No          No          No
Gi3/0/15       Disabled        0     No      No          No          No
Gi3/0/16       Disabled        0     No      No          No          No
Gi3/0/17       Disabled        0     No      No          No          No
Gi3/0/18       Disabled        0     No      No          No          No
Gi3/0/19       Disabled        0     No      No          No          No
Gi3/0/20       Disabled        0     No      No          No          No
Gi3/0/21       Disabled        0     No      No          No          No
Gi3/0/22       Disabled        0     No      No          No          No
Gi3/0/23       Disabled        0     No      No          No          No
Gi3/0/24       Disabled        0     No      No          No          No
Gi3/0/25       Disabled        0     No      No          No          No
Gi3/0/26       Disabled        0     No      No          No          No
Gi3/0/27       Disabled        0     No      No          No          No
Gi3/0/28       Disabled        0     No      No          No          No
Gi3/0/29       Disabled        0     No      No          No          No
Gi3/0/30       Disabled        0     No      No          No          No
Gi3/0/31       Disabled        0     No      No          No          No
Gi3/0/32       Disabled        0     No      No          No          No
Gi3/0/33       Disabled        0     No      No          No          No
Gi3/0/34       Disabled        0     No      No          No          No
```

```
Gi3/0/35        Disabled        0      No       No          No          No
Gi3/0/36        Disabled        0      No       No          No          No
Gi3/0/37        Disabled        0      No       No          No          No
Gi3/0/38        Disabled        0      No       No          No          No
Gi3/0/39        Disabled        0      No       No          No          No
Gi3/0/40        Disabled        0      No       No          No          No
Gi3/0/41        Disabled        0      No       No          No          No
Gi3/0/42        Disabled        0      No       No          No          No
Gi3/0/43        Disabled        0      No       No          No          No
Gi3/0/44        Disabled        0      No       No          No          No
Gi3/0/45        Disabled        0      No       No          No          No
Gi3/0/46        Disabled        0      No       No          No          No
Gi3/0/47        Disabled        0      No       No          No          No
Gi3/0/48        Disabled        0      No       No          No          No
Gi3/1/1         Disabled        0      No       No          No          No
Gi3/1/2         Disabled        0      No       No          No          No
Gi3/1/3         Disabled        0      No       No          No          No
Gi3/1/4         Disabled        0      No       No          No          No
Te3/1/1         Disabled        0      No       No          No          No
Te3/1/2         Disabled        0      No       No          No          No
Te3/1/3         Disabled        0      No       No          No          No
Te3/1/4         Disabled        0      No       No          No          No
Te3/1/5         Disabled        0      No       No          No          No
Te3/1/6         Disabled        0      No       No          No          No
Te3/1/7         Disabled        0      No       No          No          No
Te3/1/8         Disabled        0      No       No          No          No
Fo3/1/1         Disabled        0      No       No          No          No
Fo3/1/2         Disabled        0      No       No          No          No
Tw3/1/1         Disabled        0      No       No          No          No
Tw3/1/2         Disabled        0      No       No          No          No
Ap3/0/1         Disabled        0      No       No          No          No
```

Output fields are self-explanatory.

show platform software fed switch active sgacl vlan

To display global enforcement status on VLANs, use the **show platform software fed switch active sgacl vlan** command in privileged EXEC mode.

show platform software fed switch active sgacl vlan

Syntax Description

sgacl	Displays SGACL hardware information.
vlan	Specifies VLAN configuration.

Command Modes

Privileged EXEC (#)

Command History

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

Example

The following is a sample output from the **show platform software fed switch active sgacl vlan** command:

```
Device# show platform software fed switch active sgacl vlan

Enforcement enabled:
vlan0
vlan1
vlan2
vlan10
vlan102
vlan192
vlan200
```

show platform software status control-processor brief

To display brief information about CPU and memory, use the **show platform software status control-processor brief** command in privileged EXEC mode.

show platform software status control-processor brief

Syntax Description

status	Displays system status.
control-processor	Displays control processor status.
brief	Displays brief status.

Command Modes

Privileged EXEC (#)

Command History

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

Example

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

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

Load Average
 Slot  Status  1-Min  5-Min 15-Min
3-RP0 Healthy   0.03   0.07   0.04

Memory (kB)
 Slot  Status    Total     Used (Pct)     Free (Pct) Committed (Pct)
3-RP0 Healthy  7745656  4178292 (54%)  3567364 (46%)   4755060 (61%)

CPU Utilization
 Slot  CPU   User System   Nice   Idle    IRQ   SIRQ IOwait
3-RP0    0   0.50   0.40   0.00  99.10   0.00   0.00   0.00
         1   0.90   0.50   0.00  98.59   0.00   0.00   0.00
         2   0.40   0.40   0.00  99.20   0.00   0.00   0.00
         3   0.80   0.30   0.00  98.90   0.00   0.00   0.00
         4   0.60   0.30   0.00  99.09   0.00   0.00   0.00
         5   0.70   0.30   0.00  99.00   0.00   0.00   0.00
         6   1.20   0.30   0.00  98.50   0.00   0.00   0.00
         7   0.59   0.39   0.00  99.00   0.00   0.00   0.00
```

Output fields are self-explanatory.

show monitor capture <name> buffer

To display the contents of a monitor capture buffer or a capture point, use the **show monitor capture buffer** *name* **buffer** command in privileged EXEC mode.

show monitor capture *name* **buffer**

Syntax Description

buffer	Displays the contents of the specified capture buffer.
name	Represents the name of the capture buffer.

Command Modes

Privileged EXEC (#)

Command History

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

The following is sample output from the **show monitor capture***name***buffer** command:

```
Device# enable
Device# show monitor capture NewCapture buffer

Starting the packet display ........ Press Ctrl + Shift + 6 to exit

1 0.000000 10.4.1.117 -> 10.5.1.108 ICMP 124 Echo (ping) reply id=0x0008, seq=44279/63404,
 ttl=127
2 0.108862 10.4.1.113 -> 10.5.1.109 ICMP 124 Echo (ping) reply id=0x0008, seq=26717/23912,
 ttl=127
3 0.110106 10.4.1.119 -> 10.5.1.102 ICMP 124 Echo (ping) reply id=0x0008, seq=28341/46446,
 ttl=127
```

Output fields are self-explanatory.

PART III

Interface and Hardware Components

- Interface and Hardware Commands, on page 143

Interface and Hardware Commands

- bluetooth pin, on page 146
- clear coap database, on page 147
- clear macro auto configuration, on page 148
- coap endpoint (coap-proxy configuration), on page 149
- debug coap, on page 150
- device classifier, on page 151
- debug ilpower, on page 152
- debug interface, on page 153
- debug lldp packets, on page 154
- debug platform poe, on page 155
- debug platform software fed switch active punt packet-capture start, on page 156
- duplex, on page 157
- errdisable detect cause, on page 159
- errdisable recovery cause, on page 161
- errdisable recovery cause, on page 163
- interface, on page 165
- interface range, on page 167
- ip mtu, on page 169
- ipv6 mtu, on page 170
- list (coap-proxy configuration), on page 171
- lldp (interface configuration), on page 172
- logging event power-inline-status, on page 174
- macro, on page 175
- macro auto, on page 178
- macro auto apply (Cisco IOS shell scripting capability), on page 181
- macro auto config (Cisco IOS shell scripting capability), on page 183
- macro auto control, on page 184
- macro auto execute, on page 186
- macro auto global control, on page 193
- macro auto global processing, on page 195
- macro auto mac-address-group, on page 196
- macro auto processing, on page 198
- macro auto sticky, on page 199

- macro auto trigger, on page 200
- macro description, on page 201
- macro global, on page 202
- macro global description, on page 204
- max-endpoints (coap-proxy configuration), on page 205
- mdix auto, on page 206
- network-policy, on page 207
- network-policy profile (global configuration), on page 208
- port-dtls (coap-proxy configuration), on page 209
- port-unsecure (coap-proxy configuration), on page 210
- power inline, on page 211
- power inline police, on page 214
- power supply, on page 216
- resource directory (coap-proxy configuration), on page 218
- security (coap-proxy configuration), on page 219
- shell trigger, on page 220
- show beacon all, on page 221
- show coap dtls endpoints, on page 222
- show coap endpoints, on page 223
- show coap globals, on page 224
- show coap resources, on page 225
- show coap stats, on page 226
- show coap version, on page 227
- show device classifier attached, on page 228
- show device classifier clients, on page 230
- show device classifier profile type, on page 231
- show environment, on page 234
- show errdisable detect, on page 236
- show errdisable recovery, on page 238
- show ip interface, on page 239
- show interfaces, on page 244
- show interfaces counters, on page 250
- show interfaces switchport, on page 252
- show interfaces transceiver, on page 254
- show macro auto, on page 258
- show memory platform, on page 261
- show module, on page 264
- show network-policy profile, on page 265
- show parser macro, on page 266
- show platform hardware bluetooth, on page 269
- show platform hardware fed switch forward interface, on page 270
- show platform resources, on page 273
- show platform software audit, on page 274
- show platform software fed switch punt cpuq rates, on page 278
- show platform software fed switch punt packet-capture display, on page 280
- show platform software fed switch punt rates interfaces, on page 282

- show platform software ilpower, on page 285
- show platform software memory, on page 287
- show platform software process list, on page 293
- show platform software process memory, on page 297
- show platform software process slot switch, on page 300
- show platform software status control-processor, on page 302
- show platform software thread list, on page 305
- show processes cpu platform, on page 307
- show processes cpu platform history, on page 310
- show processes cpu platform monitor, on page 313
- show processes memory, on page 315
- show processes memory platform, on page 318
- show processes platform, on page 322
- show shell, on page 325
- show system mtu, on page 328
- show tech-support , on page 329
- show tech-support bgp, on page 331
- show tech-support diagnostic, on page 334
- speed, on page 336
- start (coap-proxy configuration), on page 338
- stop (coap-proxy configuration), on page 339
- switchport block, on page 340
- system mtu, on page 341
- transport (coap-proxy configuration), on page 342
- voice-signaling vlan (network-policy configuration), on page 343
- voice vlan (network-policy configuration), on page 345

bluetooth pin

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

bluetooth pin *pin*

Syntax Description

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

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

The **bluetooth pin** command can be configured either in the 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

Command	Description
show platform hardware bluetooth	Displays information about the Bluetooth interface

clear coap database

To clear the CoAP database, use the **clear coap database** command in user EXEC or privileged EXEC mode.

clear coap database

Command Default

This command has no arguments or keywords.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Example

This example shows how to clear the coap database:

```
Device(config)# clear coap database
```

clear macro auto configuration

To remove the macro applied configuration from the interfaces, use the **clear macro auto configuration** command.

Note Before executing the **clear macro auto configuration** command, you must disable Auto SmartPorts on the switch.

clear macro auto configuration {**all** | **interface** [*interface-id*]}

Syntax Description

all	Removes macro applied configuration from all the interfaces.
interface [*interface-id*]	Removes macro applied configuration from an interface.

Command Default

This command has no default setting.

Command Modes

User EXEC (>)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Use the command to remove configuration applied by macros from all the interfaces or a particular interface on the switch.

You can verify your settings by entering the **show macro auto interface** command in privileged EXEC mode.

Example

This example shows how to remove the configuration from all the switch interfaces:

```
Device(config)# clear macro auto configuration all
```

coap endpoint (coap-proxy configuration)

To configure the COAP Proxy to support multiple IPv4/IPv6 static-endpoints, use the **coap endpoint** command in coap-proxy configuration mode. To return to the default settings, use the **no** form of the command.

coap endpoint {**ipv4** | **ipv6**}[*ip-address*]
no coap endpoint {**ipv4** | **ipv6**}[*ip-address*]

Syntax Description

ipv4 *ip-address*	Specifies IPv4 static endpoint.
ipv6 *ip-address*	Specifies IPv6 static endpoint.

Command Modes

coap-proxy configuration (config-coap-proxy)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Example

This example show how to configure IPv4 static endpoint

```
Device(config)# endpoint ipv4 192.168.255.1
Device(config-coap-proxy)# transport tcp
```

debug coap

To enable debugging of the coap configurations, use the **debug coap** command in privileged EXEC mode.

debug coap {**all** | **database** | **errors** | **events** | **packet** | **trace** | **warnings**}

Syntax Description

all	Displays all coap debug messages.
database	Displays coap database debug messages.
errors	Displays coap error debug messages.
events	Displays coap event debug messages.
packet	Displays coap packet debug messages.
trace	Displays coap trace debug messages.
warnings	Displats coap warning debug messages

Command Default

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Example

The example shows how to enable debugging for coap database:

```
Device# debug coap database
```

device classifier

To enable the device classifier, use the **device classifier** command in global configuration mode. Use the **no** form of this command to disable the device classifier.

device classifier

no device classifier

Command Default

This command is disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Use the **no device classifier** command, in global configuration mode, to disable the device classifier. You cannot disable the device classifier while it is being used by features such as Auto SmartPorts (ASP).

Example

This example shows how to enable the ASP device classifier on a switch:

```
Device(config)# device classifier
Device(config)# end
```

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

Syntax Description

cdp	Displays PoE Cisco Discovery Protocol (CDP) debug messages.
event	Displays PoE event debug messages.
ha	Displays PoE high-availability 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.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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 switc 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.

debug interface {*interface-id* | **counters** {**exceptions** | **protocol memory**} | **null** *interface-number* | **port-channel** *port-channel-number* | **states** | **vlan** *vlan-id*}
no debug 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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

If you do not specify a keyword, all debug messages appear.

The **undebug interface** command is the same as the **no debug interface** command.

When you enable debugging on a switch stack, it is enabled only on the active switch. To enable debugging on a stack member, you can start a session from the active switch by using the **session** *switch-number* EXEC command. Then enter the **debug** command at the command-line prompt of the stack member. 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 commnd has no arguments or keywords.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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

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

debug platform poe

To enable debugging of a Power over Ethernet (PoE) port, use the **debug platform poe** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug platform poe [{**error** | **info**}] [**switch** *switch-number*]
no debug platform poe [{**error** | **info**}] [**switch** *switch-number*]

Syntax Description

error	(Optional) Displays PoE-related error debug messages.
info	(Optional) Displays PoE-related information debug messages.
switch *switch-number*	(Optional) Specifies the stack member. This keyword is supported only on stacking-capable switches.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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.

debug platform software fed switch active punt packet-capture start
debug platform software fed switch active punt packet-capture stop

Syntax Description

switch active	Displays information about the active switch.
punt	Specifies the punt information.
packet-capture	Specifies information about the captured packet.
start	Enables debugging of the active switch.
stop	Disables debugging of the active switch.

Command Modes

Privileged EXEC (#)

Command History

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

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 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 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 Mb/s, 10,000 Mb/s, 2.5Gb/s, or 5Gb/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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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

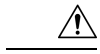
Note Half-duplex mode is supported on Gigabit Ethernet interfaces if the duplex mode is **auto** and the connected device is operating at half duplex. However, you cannot configure these interfaces to operate in half-duplex mode.

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

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

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

You can configure the duplex setting when the speed is set to **auto**.



Caution Changing the interface speed and duplex mode configuration might shut down and re-enable 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
Devic(config-if)# duplex full
```

errdisable detect cause

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

errdisable detect cause {**all** | **arp-inspection** | **bpduguard shutdown vlan** | **dhcp-rate-limit** | **dtp-flap** | **gbic-invalid** | **inline-power** | **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

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

Command Default

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

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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

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

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

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.

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** | **udld**}
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** | **udld**}

Syntax Description

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

port-mode-failure	Enables the timer to recover from the port mode change failure error-disabled state.
pppoe-ia-rate-limit	Enables the timer to recover from the PPPoE IA rate limit error-disabled state.
psecure-violation	Enables the timer to recover from a port security violation disable state.
psp	Enables the timer to recover from the protocol storm protection (PSP) error-disabled state.
security-violation	Enables the timer to recover from an IEEE 802.1x-violation disabled state.
sfp-config-mismatch	Enables error detection on an SFP configuration mismatch.
storm-control	Enables the timer to recover from a storm control error.
udld	Enables the timer to recover from the UniDirectional Link Detection (UDLD) error-disabled state.

Command Default

Recovery is disabled for all causes.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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

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

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

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

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

Examples

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

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

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** | **udld**}
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** | **udld**}

Syntax Description

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

port-mode-failure	Enables the timer to recover from the port mode change failure error-disabled state.
pppoe-ia-rate-limit	Enables the timer to recover from the PPPoE IA rate limit error-disabled state.
psecure-violation	Enables the timer to recover from a port security violation disable state.
psp	Enables the timer to recover from the protocol storm protection (PSP) error-disabled state.
security-violation	Enables the timer to recover from an IEEE 802.1x-violation disabled state.
sfp-config-mismatch	Enables error detection on an SFP configuration mismatch.
storm-control	Enables the timer to recover from a storm control error.
udld	Enables the timer to recover from the UniDirectional Link Detection (UDLD) error-disabled state.

Command Default

Recovery is disabled for all causes.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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

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

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

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

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

Examples

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

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

interface

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

interface {**AccessTunnel** *interface-number* | **Auto-Template** *interface-number* | **GigabitEthernet** *switch-number/slot-number/port-number* | **Internal Interface** *Internal Interface number* | **LISP** *interface-number* **Loopback** *interface-number* **Null** *interface-number* **Port-channel** *interface-number* **TenGigabitEthernet** *switch-number/slot-number/port-number* **TwentyFiveGigE** *switch-number/slot-number/port-number* **Tunnel** *interface-number* **Vlan** *interface-number* }

Syntax Description

AccessTunnel *interface-number*	Enables you to configure an access tunnel interface.
Auto-Template *interface-number*	Enables you to configure a auto-template interface. The range is from 1 to 999.
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.
LISP *interface-number*	Enables you to configure a LISP 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 ranges are 1 to 4, 17 to 24, and 37 to 48.

TwentyFiveGigE *switch-number/slot-number/port-number*	Enables you to configure a 25-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.
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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.
Cisco IOS XE Gibraltar 16.11.1	The **TwentyFiveGigE** keyword was added to the command.

Usage Guidelines

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

The range for uplink ports is 0-4.

The range for multi-Gigabit Ethernet ports on 24-port switches is 17-24.

The range for multi-Gigabit Ethernet ports on 48-port switches is 41-48.

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 25-Gigabit Ethernet interface

```
Device(config)# interface TwentyFiveGigE 1/1/1
Device(config-if)#
```

The following example shows how to configure a 40-Gigabit Ethernet interface

interface range

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

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

Syntax Description

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 0 to 48.
Loopback *interface-number*	Enables you to configure a loopback interface. The range is from 0 to 2147483647.
Port-channel *interface-number*	Enables you to configure a port-channel interface. The range is from 1 to 48.
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 ranges are 1 to 4, 17 to 24, and 37 to 48.
TwentyFiveGigE *switch-number/slot-number/port-number*	Enables you to configure a 25-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.
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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.
Cisco IOS XE Gibraltar 16.11.1	The **TwentyFiveGigE** keyword was added to the command.

Usage Guidelines

The range for uplink ports is 0-4.

The range for multi-Gigabit Ethernet ports on 24-port switches is 17-24.

The range for multi-Gigabit Ethernet ports on 48-port switches is 41-48.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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

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

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

The following example sets the maximum IP packet size for VLAN 200 to 1000 bytes:

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

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

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

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

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

<output truncated>
```

ipv6 mtu

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

ipv6 mtu *bytes*
no ipv6 mtu *bytes*

Syntax Description

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

Command Default

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

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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

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

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

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

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

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

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

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

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

<output truncated>
```

list (coap-proxy configuration)

To restrict the IP address range where the lights and their resources can be learnt, use the **list** command in coap-proxy configuration mode. To return to the default settings, use the **no** form of the command.

A maximum of five ip-lists can be configured, irrespective of ipv4 or ipv6, using the **list** command.

list {**ipv4** | **ipv6**}[*list-name*]
no list {**ipv4** | **ipv6**}[*list-name*]

Syntax Description

ipv4 *list-name*	Specifies IPv4 list name.
ipv6 *list-name*	Specifies IPv6 list name.

Command Modes

coap-proxy configuration (config-coap-proxy)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

To access coap-proxy configuration mode, enter the **coap proxy** command in global configuration mode.

Example

This example shows how to restrict the IPv4 address range using a list name.

```
Device(config)# coap proxy
Device config-coap-proxy)# list ipv4 trial_list
```

lldp (interface configuration)

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

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

Syntax Description

med-tlv-select	Selects an LLDP Media Endpoint Discovery (MED) time-length-value (TLV) element to send.
tlv	String that identifies the TLV element. Valid values are the following: • **inventory-management**— LLDP MED Inventory Management TLV. • **location**— LLDP MED Location TLV. • **network-policy**— LLDP MED Network Policy TLV. • **power-management**— LLDP MED Power Management TLV.
receive	Enables the interface to receive LLDP transmissions.
tlv-select	Selects the LLDP TLVs to send.
power-management	Sends the LLDP Power Management TLV.
transmit	Enables LLDP transmission on the interface.

Command Default

LLDP is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

This command is supported on 802.1 media types.

If the interface is configured as a tunnel port, LLDP is automatically disabled.

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

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

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

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

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

logging event power-inline-status

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

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

Syntax Description

This command has no arguments or keywords.

Command Default

Logging of PoE events is enabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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

Examples

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

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

macro

To apply a macro to an interface or to apply and debug a macro on an interface, use the **macro** command in interface configuration mode.

macro {**apply** | **trace**}*macro-name* [**parameter** {*value*}][**parameter** {*value*}][**parameter** {*value*}]

Syntax Description

apply	Applies a macro to an interface.
trace	Applies a macro to an interface and then debugs it.
macro-name	Specifies the name of the macro.
parameter *value*	(Optional) Specifies unique parameter values that are specific to the interface. You can enter up to three keyword-value pairs. Parameter keyword matching is case sensitive. All matching occurrences of the keyword are replaced with the corresponding value.

Command Default

This command has no default setting.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

You can use the **macro apply** *macro-name* command to apply and show the macros running on an interface.

You can use the **macro trace** *macro-name* command to apply and then debug the macro to find any syntax or configuration errors.

If a command fails because of a syntax error or a configuration error when you apply a macro, the macro continues to apply the remaining commands to the interface.

When creating a macro that requires the assignment of unique values, use the **parameter** *value* keywords to designate values specific to the interface.

Keyword matching is case sensitive. All matching occurrences of the keyword are replaced with the corresponding value. Any full match of a keyword, even if it is part of a larger string, is considered a match and is replaced by the corresponding value.

Some macros might contain keywords that require a parameter value. You can use the **macro apply** *macro-name* ? command to display a list of any required values in the macro. If you apply a macro without entering the keyword values, the commands are invalid and are not applied.

There are Cisco-default SmartPorts macros embedded in the switch software. You can display these macros and the commands that they contain by using the **show parser macro** command in user EXEC mode.

Follow these guidelines when you apply a Cisco-default SmartPorts macro on an interface:

- Display all macros on the switch by using the **show parser macro** command in user EXEC mode. Display the contents of a specific macro by using the **show parser macro** *macro-name* command in user EXEC mode.
- Keywords that begin with $ mean that a unique parameter value is required. Append the Cisco-default macro with the required values by using the **parameter** *value* keywords.

The Cisco-default macros use the $ character to identify required keywords. You can use the $ character to define keywords when you create a macro.

When you apply a macro to an interface, the macro name is automatically added to the interface. You can display the applied commands and macro names by using the **show running-config interface** *interface-id* command in user EXEC mode.

A macro applied to an interface range behaves the same way as a macro applied to a single interface. When you use an interface range, the macro is applied sequentially to each interface within the range. If a macro command fails on one interface, it is still applied to the remaining interfaces.

You can delete a macro-applied configuration on an interface by entering the **default interface** *interface-id* command in interface configuration mode.

Example

After you use the **macro name** command, in interface configuration mode, you can apply it to an interface. This example shows how to apply a user-created macro called duplex to an interface:

```
Device(config-if)# macro apply duplex
```

To debug a macro, use the **macro trace** command, in interface configuration mode, to find any syntax or configuration errors in the macro as it is applied to an interface.

```
Device(config-if)# macro trace duplex
Applying command...'duplex auto'
%Error Unknown error.
Applying command...'speed nonegotiate'
```

This example shows how to display the Cisco-default cisco-desktop macro and how to apply the macro and set the access VLAN ID to 25 on an interface:

```
Device# show parser macro cisco-desktop
-------------------------------------------------------------
Macro name : cisco-desktop
Macro type : default
# Basic interface - Enable data VLAN only
# Recommended value for access vlan (AVID) should not be 1
switchport access vlan $AVID
switchport mode access
# Enable port security limiting port to a single
# MAC address -- that of desktop
switchport port-security
switchport port-security maximum 1
# Ensure port-security age is greater than one minute
# and use inactivity timer
switchport port-security violation restrict
switchport port-security aging time 2
switchport port-security aging type inactivity
# Configure port as an edge network port
spanning-tree portfast
```

```
spanning-tree bpduguard enable
------------------------------------------------------------------
Device#
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# interface gigabitethernet1/0/4
Device(config-if)# macro apply cisco-desktop $AVID 25
```

macro auto

To configure and apply a global macro using the CLI, use the **macro auto** command in privileged EXEC mode.

Use the **no** form of this command to return to the default setting.

macro auto {**apply** | **config**} *macro-name*

Syntax Description

apply	Applies the macro.
config	Enters the macro parameters.
macro-name	Specifies the macro name.

Command Default

No macros are applied to the switch.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

To remove the macro from the switch, enter the **no** forms of the macro commands.

If you enter the **macro auto config** *macro-name* command, you are prompted to enter values for all the macro parameters.

Use the exact text string when entering the macro-name. The entries are case sensitive.

The user-defined values appear only in the **show macro auto** or **show running-config** command output.

Example

This example shows how to display global macros:

```
Device# macro auto apply ?
CISCO_SWITCH_AAA_ACCOUNTING         Configure aaa accounting parameters
CISCO_SWITCH_AAA_AUTHENTICATION     Configure aaa authentication parameters
CISCO_SWITCH_AAA_AUTHORIZATION      Configure aaa authorization parameters
CISCO_SWITCH_AUTO_IP_CONFIG         Configure the ip parameters
CISCO_SWITCH_AUTO_PCI_CONFIG        Configure PCI compliant parameters
CISCO_SWITCH_DOMAIN_NAME_CONFIG     Configure domain name
CISCO_SWITCH_ETHERCHANNEL_CONFIG    Configure the etherchannel parameters
CISCO_SWITCH_HOSTNAME_CONFIG        Configure hostname
CISCO_SWITCH_HTTP_SERVER_CONFIG     Configure http server
CISCO_SWITCH_LOGGING_SERVER_CONFIG  Configure logging server
CISCO_SWITCH_MGMT_VLAN_CONFIG       Configure management vlan parameters
CISCO_SWITCH_NAME_SERVER_CONFIG     Configure name server parameters
CISCO_SWITCH_NTP_SERVER_CONFIG      Configure NTP server
CISCO_SWITCH_RADIUS_SERVER_CONFIG   Configure radius server
CISCO_SWITCH_SETUP_SNMP_TRAPS       Configure SNMP trap parameters
CISCO_SWITCH_SETUP_USR_CONFIG       Configure the user parameters
CISCO_SWITCH_SNMP_SOURCE_CONFIG     Configure snmp source interface
```

```
CISCO_SWITCH_TACACS_SERVER_CONFIG   Configure tacacs server
CISCO_SWITCH_USER_PASS_CONFIG       Configure username and password

Device# macro auto config ?
CISCO_SWITCH_AAA_ACCOUNTING         Configure aaa accounting parameters
CISCO_SWITCH_AAA_AUTHENTICATION     Configure aaa authentication parameters
CISCO_SWITCH_AAA_AUTHORIZATION      Configure aaa authorization parameters
CISCO_SWITCH_AUTO_IP_CONFIG         Configure the ip parameters
CISCO_SWITCH_AUTO_PCI_CONFIG        Configure PCI compliant parameters
CISCO_SWITCH_DOMAIN_NAME_CONFIG     Configure domain name
CISCO_SWITCH_ETHERCHANNEL_CONFIG    Configure the etherchannel parameters
CISCO_SWITCH_HOSTNAME_CONFIG        Configure hostname
CISCO_SWITCH_HTTP_SERVER_CONFIG     Configure http server
CISCO_SWITCH_LOGGING_SERVER_CONFIG  Configure logging server
CISCO_SWITCH_MGMT_VLAN_CONFIG       Configure management vlan parameters
CISCO_SWITCH_NAME_SERVER_CONFIG     Configure name server parameters
CISCO_SWITCH_NTP_SERVER_CONFIG      Configure NTP server
CISCO_SWITCH_RADIUS_SERVER_CONFIG   Configure radius server
CISCO_SWITCH_SETUP_SNMP_TRAPS       Configure SNMP trap parameters
CISCO_SWITCH_SETUP_USR_CONFIG       Configure the user parameters
CISCO_SWITCH_SNMP_SOURCE_CONFIG     Configure snmp source interface
CISCO_SWITCH_TACACS_SERVER_CONFIG   Configure tacacs server
CISCO_SWITCH_USER_PASS_CONFIG       Configure username and password
```

This example shows how to display the parameters for a specific macro:

```
Device# macro auto config CISCO_SWITCH_AUTO_IP_CONFIG ?
CISCO_SWITCH_DOMAIN_NAME_CONFIG     domain name parameters
CISCO_SWITCH_LOGGING_SERVER_CONFIG  logging host parameters
CISCO_SWITCH_NAME_SERVER_CONFIG     name server parameters
CISCO_SWITCH_NTP_SERVER_CONFIG      ntp server parameters
LINE                                Provide parameters of form [Parameters
                                    name=value]
<cr>

Device# macro auto config CISCO_SWITCH_AUTO_PCI_CONFIG ?
CISCO_SWITCH_AAA_ACCOUNTING         aaa accounting parameters
CISCO_SWITCH_AAA_AUTHENTICATION     aaa authentication parameters
CISCO_SWITCH_AAA_AUTHORIZATION      aaa authorization parameters
CISCO_SWITCH_HTTP_SERVER_CONFIG     http server parameters
CISCO_SWITCH_RADIUS_SERVER_CONFIG   radius server parameters
CISCO_SWITCH_TACACS_SERVER_CONFIG   tacacs server parameters
LINE                                Provide parameters of form [Parameters
                                    name=value]
<cr>

Device# macro auto config CISCO_SWITCH_SETUP_SNMP_TRAPS ?
CISCO_SWITCH_SNMP_SOURCE_CONFIG     snmp source parameters
LINE                                Provide parameters of form [Parameters
                                    name=value]
<cr>

Device# macro auto config CISCO_SWITCH_SETUP_USR_CONFIG ?CISCO_AUTO_TIMEZONE_CONFIG timezone
 parameters
CISCO_SWITCH_HOSTNAME_CONFIG        hostname parameter
LINE                                Provide parameters of form [Parameters
                                    name=value]
<cr>
```

This example shows how to set macro parameters and apply the macro using the CLI:

```
Device# macro auto config CISCO_SWITCH_ETHERCHANNEL_CONFIG
Enter the port channel id[1-48] for 3K & 2350,[1-6] for 2K: 2
Enter the port channel type, Layer:[2-3(L3 not supported on 2K)]: 2
Enter etherchannel mode for the interface[auto/desirable/on/active/passive]: active
Enter the channel protocol[lacp/none]: lacp
Enter the number of interfaces to join the etherchannel[8-PAGP/MODE:ON,16-LACP]: 7
Enter interface name[GigabitEthernet3/0/3]: gigabitethernet1/0/1
Enter interface name[GigabitEthernet3/0/3]: gigabitethernet1/0/2
Enter interface name[GigabitEthernet3/0/3]: gigabitethernet1/0/3
Enter interface name[GigabitEthernet3/0/3]: gigabitethernet1/0/4
Enter interface name[GigabitEthernet3/0/3]: gigabitethernet1/0/5
Enter interface name[GigabitEthernet3/0/3]: gigabitethernet1/0/6
Enter interface name[GigabitEthernet3/0/3]: gigabitethernet1/0/7
Do you want to apply the parameters? [yes/no]: yes
Enter configuration commands, one per line. End with CNTL/Z.
Enter configuration commands, one per line. End with CNTL/Z.
Enter configuration commands, one per line. End with CNTL/Z.
Enter configuration commands, one per line. End with CNTL/Z.
Enter configuration commands, one per line. End with CNTL/Z.
Enter configuration commands, one per line. End with CNTL/Z.
Enter configuration commands, one per line. End with CNTL/Z.
Device# macro auto apply CISCO_SWITCH_ETHERCHANNEL_CONFIG
Enter configuration commands, one per line. End with CNTL/Z.
Device#
```

macro auto apply (Cisco IOS shell scripting capability)

To configure and apply a global macro using the Cisco IOS shell scripting capability, use the **macro auto apply** command in privileged EXEC mode. Use the **no** form of this command to return to the default setting.

macro auto apply *macro-name*

Syntax Description

apply	Applies the macro.
macro-name	Specifies the macro name.

Command Default

No macros are applied to the switch.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

To remove the macro from the switch, enter the **no** forms of the macro commands.

Use the exact text string when entering the *macro-name*. The entries are case sensitive.

The user-defined values appear only in the **show macro auto** or **show running-config** command output.

You can also use the Cisco IOS shell scripting capability to set the parameters. For examples, see the

"Configuring and Applying Global Macros" section in the "Configuring Auto Smartports and Static Smartports Macros" chapter.

Example

This example shows how to display global macros:

```
Device# macro auto apply ?

CISCO_SWITCH_AAA_ACCOUNTING         Configure aaa accounting parameters
CISCO_SWITCH_AAA_AUTHENTICATION     Configure aaa authentication parameters
CISCO_SWITCH_AAA_AUTHORIZATION      Configure aaa authorization parameters
CISCO_SWITCH_AUTO_IP_CONFIG         Configure the ip parameters
CISCO_SWITCH_AUTO_PCI_CONFIG        Configure PCI compliant parameters
CISCO_SWITCH_DOMAIN_NAME_CONFIG     Configure domain name
CISCO_SWITCH_ETHERCHANNEL_CONFIG    Configure the etherchannel parameters
CISCO_SWITCH_HOSTNAME_CONFIG        Configure hostname
CISCO_SWITCH_HTTP_SERVER_CONFIG     Configure http server
CISCO_SWITCH_LOGGING_SERVER_CONFIG  Configure logging server
CISCO_SWITCH_MGMT_VLAN_CONFIG       Configure management vlan parameters
CISCO_SWITCH_NAME_SERVER_CONFIG     Configure name server parameters
CISCO_SWITCH_NTP_SERVER_CONFIG      Configure NTP server
CISCO_SWITCH_RADIUS_SERVER_CONFIG   Configure radius server
CISCO_SWITCH_SETUP_SNMP_TRAPS       Configure SNMP trap parameters
CISCO_SWITCH_SETUP_USR_CONFIG       Configure the user parameters
CISCO_SWITCH_SNMP_SOURCE_CONFIG     Configure snmp source interface
```

```
CISCO_SWITCH_TACACS_SERVER_CONFIG   Configure tacacs server
CISCO_SWITCH_USER_PASS_CONFIG       Configure username and password
```

macro auto config (Cisco IOS shell scripting capability)

To configure and apply a global macro, use the **macro auto config** command in privileged EXEC mode. Use the **no** form of this command to return to the default setting.

macro auto config *macro-name* [*parameter=value* [*parameter=value*]**...**]

Syntax Description

config	Enters the macro parameters.
macro-name	Specifies the macro name.
parameter=value [parameter=value] ...	*parameter=value*—Replaces values for global macro parameter values. Enter values in the form of name value pair separated by a space: <name1>=<value1> [<name2>=<value2>...]

Command Default

No macros are applied to the switch.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

To remove the macro from the switch, enter the **no** forms of the macro commands.

If you enter the **macro auto config** *macro-name* command, you are prompted to enter values for all the macro parameters.

Use the exact text string when entering the *macro-name* and *parameters*. The entries are case sensitive.

The user-defined values appear only in the **show macro auto** or **show running-config** command output.

You can also use the Cisco IOS shell scripting capability to set the parameters. For examples, see the "Configuring and Applying Global Macros" section in the "Configuring Auto Smartports and Static Smartports Macros" chapter.

macro auto control

To specify when the switch applies an Auto Smartports macro based on the detection method, device type, or trigger (referred to as event trigger control), use the **macro auto control** command in interface configuration mode. Use the **no** form of this command to disable trigger-to-macro mapping. The switch then does not apply macros based on event triggers.

macro auto control {**detection** [**cdp**] [**lldp**] [**mac-address**] | **device** [**ip-camera**] [**media-player**] [**phone**] [**lightweight-ap**] [**access-point**] [**router**] [**switch**] | **trigger** [**last-resort**]}
no macro auto control {**detection** [**cdp**] [**lldp**] [**mac-address**] | **device** [**ip-camera**] [**media-player**] [**phone**] [**lightweight-ap**] [**access-point**] [**router**] [**switch**] | **trigger** [**last-resort**]}

Syntax Description

detection [cdp] [lldp] [mac-address]	detection—Sets one or more of these as an event trigger: • (Optional) **cdp**—CDP messages • (Optional) **lldp**—LLDP messages • (Optional) **mac-address**—User-defined MAC address groups
device [access-point] [ip-camera] [lightweight-ap] [media-player] [phone] [router] [switch]	device—Sets one or more of these devices as an event trigger: • (Optional) **access-point**—Autonomous access point • (Optional) **ip-camera**—Cisco IP video surveillance camera • (Optional) **lightweight-ap**—Lightweight access point • (Optional) **media-player**—Digital media player • (Optional) **phone**—Cisco IP phone • (Optional) **router**—Cisco router • (Optional) **switch**—Cisco switch
trigger [last-resort]	trigger—Sets a specific event trigger. • (Optional) **last-resort**—Last-resort trigger.

Command Default

The switch uses the device type as the event trigger. If the switch cannot determine the device type, it uses MAC address groups, MAB messages, 802.1x authentication messages, and LLDP messages in random order.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

If you do not set event triggers, the switch uses the device type as the event trigger. If the switch cannot determine the device type, it uses MAC address groups, MAB messages, 802.1x authentication messages, and LLDP messages in random order.

To verify that a macro is applied to an interface, use the **show macro auto interface** command in user EXEC mode.

Example

This example shows how to set LLDP messages and MAC address groups as event triggers:

```
Device(config)# interface gigabitethernet 5/0/2
Device(config-if)# macro auto control detection lldp mac-address
Device(config-if)# exit
Device(config)# end
```

This example shows how to set access points, video surveillance cameras, and digital media players as event triggers:

Note The switch applies a built-in macro only when it detects an access point, video surveillance camera, or digital media player.

```
Device(config)# interface gigabitethernet 5/0/1
Device(config-if)# macro auto control device access-point ip-camera media-player
Device(config-if)# exit
Device(config)# end
```

macro auto execute

To replace built-in macro default values and to configure mapping from an event trigger to a built-in or user-defined macro, use the **macro auto execute** command in global configuration mode.

macro auto execute *event trigger* {**builtin** *built-in macro* | **remote** *url*} {*parameter=value*} {*function contents*}
no macro auto execute *event trigger* {**builtin** *built-in macro* | **remote** *url*} {*parameter=value*} {*function contents*}

Syntax Description

event trigger	Defines mapping from an event trigger to a built-in macro. Specifies an event trigger: • CISCO_CUSTOM_EVENT • CISCO_DMP_EVENT • CISCO_IPVSC_EVENT • CISCO_LAST_RESORT_EVENT • CISCO_PHONE_EVENT • CISCO_ROUTER_EVENT • CISCO_SWITCH_EVENT • CISCO_WIRELESS_AP_EVENT • CISCO_WIRELESS_LIGHTWEIGHT_AP_EVENT • WORD—Apply a user-defined event trigger such as a MAC address group

builtin *built-in macro name*	(Optional) Specifies a builtin built-in macro name: • CISCO_AP_AUTO_SMARTPORT Specify the parameter value: NATIVE_VLAN=1 • CISCO_DMP_AUTO_SMARTPORT Specify the parameter value: ACCESS_VLAN=1. • CISCO_IPVSC_AUTO_SMARTPORT Specify the parameter value: ACCESS_VLAN=1. • CISCO_LWAP_AUTO_SMARTPORT Specify the parameter value: ACCESS_VLAN=1. • CISCO_PHONE_AUTO_SMARTPORT Specify the parameter values: ACCESS_VLAN=1 and VOICE_VLAN=2. • CISCO_ROUTER_AUTO_SMARTPORT Specify the parameter value: NATIVE_VLAN=1. • CISCO_SWITCH_AUTO_SMARTPORT Specify the parameter value: NATIVE_VLAN=1.
parameter=value	(Optional) *parameter=value*—Replaces default values for parameter values shown for the *bultin-macro name*, for example, ACCESS_VLAN=1. Enter new values in the form of name value pair separated by a space: [<name1>=<value1> <name2>=<value2>...].
{function contents}	(Optional) *{function contents}*— Specifies a user-defined macro to associate with the trigger. Enter the macro contents within braces. Begin the Cisco IOS shell commands with the left brace and end the command grouping with the right brace.

remote *url*	(Optional) Specifies a remote server location: • The syntax for the local flash file system on the standalone switch or the stack's active switch: **flash**: The syntax for the local flash file system on a stack member: **flash** *member number*: The syntax for the FTP: **ftp**:[[//*username*[:*password*]@*location*]/*directory*]/*filename* The syntax for an HTTP server: **http**://[[*username*:*password*]@]{*hostname* | *host-ip*}[/*directory*]/*filename* The syntax for a secure HTTP server: **https**://[[*username*:*password*]@]{*hostname* | *host-ip*}[/*directory*]/*filename* The syntax for the NVRAM: **nvram**://[[*username*:*password*]@][/*directory*]/*filename* The syntax for the Remote Copy Protocol (RCP): **rcp**:[[//*username@location*]/*directory*]/*filename* The syntax for the Secure Copy Protocol (SCP): **scp**:[[//*username@location*]/*directory*]/*filename* The syntax for the TFTP: **tftp**:[[//*location*]/*directory*]/*filename*

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Use the **macro auto execute** command to replace the built-in macro default values with values that are specific to your switch.

The switch automatically maps from event triggers to built-in macros. The built-in macros are system-defined macros in the software image. You can also create user-defined macros by using the Cisco IOS shell scripting capability.

You can create new event triggers by using the **shell trigger** commands in global configuration mode. Use the **show shell triggers** command in privileged EXEC to display the contents of the user-defined triggers and macros.

You can use the **macro auto mac-address-group** command in global configuration mode to create event triggers for devices that do not support Cisco Discovery Protocol (CDP) or Link Layer Discovery Protocol (LLDP).

You can use the remote macro feature to store macros in a central location for designated network switches to use. You can then maintain and update the macro files for use by multiple switches. Use **remote** *url* to configure the remote server location and macro path information. There are no specific file extension requirements for saved macro files.

Auto Smartports macros and antimacros (the antimacro is the portion of the applied macro that removes it at link down) have these guidelines and limitations:

- You can delete or change the built-in macros. However, you can override a built-in macro by creating a user-defined macro with the same name. To restore the original built-in macro, delete the user-defined macro.
- If you enable both the **macro auto device** and the **macro auto execute** commands, the parameters specified in the command last executed are applied to the switch. Only one command is active on the switch.
- To avoid system conflicts when macros are applied, remove all port configurations except for 802.1x authentication.
- Do not configure port security when enabling Auto SmartPorts on the switch.
- If the macro conflicts with the original configuration, either the macro does not apply some of the original configuration commands, or the antimacro does not remove them. (The antimacro is the portion of the applied macro that removes the macro at a link-down event.)
- For example, if 802.1x authentication is enabled, you cannot remove the switchport-mode access configuration. Remove the 802.1x authentication before removing the switchport mode configuration.
- A port cannot be a member of an EtherChannel when you apply Auto SmartPorts macros.
- The built-in-macro default data VLAN is VLAN 1. The default voice VLAN is VLAN 2. If your switch uses different access, native, or voice VLANs, use the **macro auto device** or the **macro auto execute** commands to configure the values.
- For 802.1x authentication or MAC authentication bypass (MAB), to detect non-Cisco devices, configure the RADIUS server to support the Cisco attribute-value pair **auto-smart-port=***event trigger*
- The switch supports Auto SmartPort macros only on directly connected devices. Multiple device connections, such as hubs, are not supported.
- If authentication is enabled on a port, the switch ignores a MAC address trigger if authentication fails.
- The order of CLI commands within the macro and the corresponding antimacro can be different.

.

Example

This example shows how to use two built-in macros for connecting Cisco switches and Cisco IP phones to the switch. This example modifies the default voice VLAN, access VLAN, and native VLAN for the trunk interface:

```
Device(config)# !!! the next command modifies the access and voice vlans
Device(config)# !!! for the built in Cisco IP phone auto smartport macro
Device(config)# macro auto execute CISCO_PHONE_EVENT builtin CISCO_PHONE_AUTO_SMARTPORT
ACCESS_VLAN=10 VOICE_VLAN=20
Device(config)# !!! the next command modifies the Native vlan used for inter switch trunks
```

```
Device(config)# macro auto execute CISCO_SWITCH_EVENT builtin CISCO_SWITCH_AUTO_SMARTPORT
NATIVE_VLAN=10
Device(config)# !!! the next command enables auto smart ports globally
Device(config)# macro auto global processing
Device(config)# exit
Device# !!! here is the running configuration of the interface connected
Device# !!! to another Cisco Switch after the Macro is applied
Device# show running-config interface gigabitethernet1/0/1
Building configuration...

Current configuration : 284 bytes
!
interface GigabitEthernet1/0/1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 10
 switchport mode trunk
 srr-queue bandwidth share 10 10 60 20
 queue-set 2
 priority-queue out
 mls qos trust cos
 auto qos voip trust
 macro description CISCO_SWITCH_EVENT
end
```

This example shows how to map a user-defined event trigger called media player to a user-defined macro

1. Connect the media player to an 802.1x- or MAB-enabled switch port.
2. On the RADIUS server, set the attribute-value pair to auto-smart-port=DMP_EVENT
3. On the switch, create the event trigger DMP_EVENT, and enter the user-defined macro commands.
4. The switch recognizes the attribute-value pair=DMP_EVENT response from the RADIUS server and applies the macro associated with this event trigger.

```
Device(config)# shell trigger DMP_EVENT mediaplayer
Device(config)# macro auto execute DMP_EVENT {
if [[ $LINKUP == YES ]]; then
conf t
 interface $INTERFACE
   macro description $TRIGGER
   switchport access vlan 1
   switchport mode access
   switchport port-security
   switchport port-security maximum 1
   switchport port-security violation restrict
   switchport port-security aging time 2
   switchport port-security aging type inactivity
   spanning-tree portfast
   spanning-tree bpduguard enable
   exit
fi
if [[ $LINKUP == NO ]]; then
conf t
interface $INTERFACE
     no macro description $TRIGGER
     no switchport access vlan 1
     if [[ $AUTH_ENABLED == NO ]]; then
        no switchport mode access
     fi
```

```
     no switchport port-security
     no switchport port-security maximum 1
     no switchport port-security violation restrict
     no switchport port-security aging time 2
     no switchport port-security aging type inactivity
     no spanning-tree portfast
     no spanning-tree bpduguard enable
     exit
fi
```

Table 12: Supported Cisco IOS Shell Keywords

Command	Description
{	Begin the command grouping.
}	End the command grouping.
[[	Use as a conditional construct.
]]	Use as a conditional construct.
else	Use as a conditional construct.
==	Use as a conditional construct.
fi	Use as a conditional construct.
if	Use as a conditional construct.
then	Use as a conditional construct.
-z	Use as a conditional construct.
$	Variables that begin with the $ character are replaced with a parameter value.
#	Use the # character to enter comment text.

Table 13: Unsupported Cisco IOS Shell Reserved Keywords

Command	Description
|	Pipeline.
case	Conditional construct.
esac	Conditional construct.
for	Looping construct.
function	Shell function.
in	Conditional construct.
select	Conditional construct.

Command	Description
time	Pipeline.
until	Looping construct.
while	Looping construct.

macro auto global control

To specify when the switch applies an Auto Smartports macro based on the device type or trigger (referred to as event trigger control), use the **macro auto global control** command in global configuration mode. Use the **no** form of this command to disable trigger-to-macro mapping.

macro auto global control {**detection** [**cdp**] [**lldp**][**mac-address**] | **device** [**access-point**] [**ip-camera**] [**lightweight-ap**] [**media-player**] [**phone**] [**router**] [**switch**] | **trigger** [**last-resort**]}
no macro auto global control {**detection** [**cdp**] [**lldp**] [**mac-address**] | **device** [**access-point**] [**ip-camera**] [**lightweight-ap**] [**media-player**] [**phone**] [**router**] [**switch**] | **trigger** [**last-resort**]}

Syntax Description

detection [cdp] [lldp] [mac-address]	detection—Sets one or more of these as an event trigger: • (Optional) **cdp**—CDP messages • (Optional) **lldp**—LLDP messages • (Optional) **mac-address**—User-defined MAC address groups
device [access-point] [ip-camera] [lightweight-ap] [media-player] [phone] [router] [switch]	device—Sets one or more of these devices as an event trigger: • (Optional) **access-point**—Autonomous access point • (Optional) **ip-camera**—Cisco IP video surveillance camera • (Optional) **lightweight-ap**—Lightweight access point • (Optional) **media-player**—Digital media player • (Optional) **phone**—Cisco IP phone • (Optional) **router**—Cisco router • (Optional) **switch**—Cisco switch
trigger [last-resort]	trigger—Sets a specific event trigger. • (Optional) **last-resort**—Last-resort trigger.

Command Default

The switch uses the device type as the event trigger. If the switch cannot determine the device type, it uses MAC address groups, MAB messages, 802.1x authentication messages, and LLDP messages in random order.

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines If you do not set event triggers, the switch uses the device type as the event trigger. If the switch cannot determine the device type, it uses MAC address groups, MAB messages, 802.1x authentication messages, and LLDP messages in random order.

To verify that a macro is applied to a switch, use the **show macro auto global** command in user EXEC mode.

Example

This example shows how to set CDP messages, LLDP messages and MAC address groups as event triggers:

```
Device(config)# macro auto global control detection cdp lldp mac-address
Device(config)# end
```

This example shows how to set autonomous access points, lightweight access points, and IP phones:

```
Device(config)# macro auto global control device access-point lightweight-ap phone
Device(config)# end
```

macro auto global processing

To enable Auto SmartPorts macros on the switch, use the **macro auto global processing** command in global configuration mode. Use the **no** form of this command to disable the macros.

macro auto global processing

no macro auto global processing

Command Default

Auto Smartports is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Use the **macro auto global processing** command to globally enable macros on the switch. To disable macros on a specific port, use the **no macro auto processing** command in interface mode.

When using 802.1x or MAB authentication, you need to configure the RADIUS server to support the Cisco attribute-value pair **auto-smart-port**=*event trigger*. If authentication fails, the macro is not applied. If the 802.1x or MAB authentication fails on the interface, the switch does not use the fallback CDP event trigger.

When CDP-identified devices advertise multiple capabilities, the switch chooses a capability first by switch and then by router.

To verify that a macro is applied to an interface, use the **show macro auto interface**command in privileged EXEC mode.

Example

This example shows how to enable Auto SmartPorts on the switch and to disable the feature on a specific interface:

```
Device(config)# macro auto global processing
Device(config)# interface gigabitethernet 0/1
Device(config-if)# no macro auto processing
Device(config-if)# exit
Device(config)#
```

macro auto mac-address-group

To create an event trigger for devices that do not support Cisco Discovery Protocol (CDP) or Link Layer Discover Protocol (LLDP), use the **macro auto mac-address-group** command in global configuration mode. Use the **no** form of this command to delete the group.

macro auto mac-address-group *name* {**mac-address list** *list* | **oui** {**list** *list* | **range** *start-value* **size** *number*}}
no macro auto mac-address-group *name* {**mac-address list** *list* | **oui** {**list** *list* | **range** *start-value* **size** *number*}}

Syntax Description

name	Specifies the group name.
ui	(Optional) Specifies an operationally unique identifier (OUI) **list** or **range**. • **list**—Enter an OUI list in hexadecimal format separated by spaces. • **range**—Enter the starting OUI hexadecimal value (*start-value*). • **size**—Enter the length of the range (number) from 1 to 5 to create a list of sequential addresses.
mac-address list *list*	(Optional) Configures a list of MAC addresses separated by a space.

Command Default

No groups are defined.

Command Modes

Group configuration (config-addr-grp-mac)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Use the **macro auto mac-address-group** command to create an event trigger for devices that do not support CDP or LLDP. Use the MAC address group as a trigger to map to a built-in or user-defined macro by using the **macro auto execute** command. At link-up the switch detects the device type and applies the specified macro.

The switch supports up to ten MAC address groups. Each group can have up to 32 OUI and 32 MAC configured addresses.

Example

This example shows how to create a MAC-address-group event trigger called *address_trigger* and how to verify your entries:

```
Device(config)# macro auto mac-address-group mac address_trigger
Device(config-addr-grp-mac)# mac-address list 2222.3333.3334 22.33.44 a.b.c
Device(config-addr-grp-mac)# oui list 455555 233244
```

```
Device(config-addr-grp-mac)# oui range 333333 size 2
Device(config-addr-grp-mac)# exit
Device(config)# end
Device# show running configuration
!
!macro auto mac-address-group address_trigger
 oui list 333334
 oui list 333333
 oui list 233244
 oui list 455555
 mac-address list 000A.000B.000C
 mac-address list 0022.0033.0044
 mac-address list 2222.3333.3334
!

<output truncated>
```

macro auto processing

To enable Auto SmartPorts macros on an interface, use the **macro auto processing** command in interface configuration mode. Use the no form of this command to disable the macros.

macro auto processing

no macro auto processing

Command Default

Auto SmartPorts is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Use the **macro auto processing** command, in interface configuration mode, to enable macros on a specific interface. To disable macros on a specific interface, use the no macro auto processing command, in interface configuration mode.

A port cannot be a member of an EtherChannel when you apply Auto SmartPorts macros. If you use EtherChannels, disable Auto SmartPorts on the EtherChannel interface by using the **no macro auto processing** command. The EtherChannel interface applies the configuration to the member interfaces.

To verify that a macro is applied to an interface, use the **show macro auto interface** command in privileged EXEC mode.

Example

This example shows how to enable Auto SmartPorts on the switch and to disable the feature on a specific interface:

```
Device(config)# interface gigabitethernet 0/1
Device(config-if)# no macro auto processing
Device(config-if)# exit
Device(config)# macro auto global processing
```

macro auto sticky

To configure macros to remain active after a link-down event, referred to as macro persistence, use the **macro auto sticky** command in global configuration mode. Use the **no** form of this command to disable the macro persistence.

macro auto sticky
no macro auto sticky

Command Default

Macro persistence is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Use the **macro auto sticky** command so that macros remain active after a link-down event.

Example

This example shows how to enable macro persistence on an interface:

```
Device(config)# interface gigabitethernet 5/0/2
Device(config-if)# macro auto port sticky
Device(config-if)# exit
Device(config)# end
```

macro auto trigger

To enter the configure-macro-trigger mode and define a trigger for a device that has no built-in trigger and associate the trigger with a device or profile, use the **macro auto trigger** command in global configuration mode. To remove the user-defined trigger, use the **no** form of this command.

macro auto trigger *trigger_name* {**device** | **exit** | **no** | **profile**}
no macro auto trigger *trigger_name* {**device** | **exit** | **no** | **profile**}

Syntax Description

trigger_name	Specifies a trigger to be associated with the device type or profile name.
device	Specifies a device name to map to the named trigger.
exit	Exits device group configuration mode.
no	Removes any configured device.
profile	Specifies a profile name to map to the named trigger.

Command Default

No user-defined triggers are configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

If a device is classified by the Device Classifier, but does not have a built-in trigger defined, use the **macro auto trigger** command, in global configuration mode, to define a trigger based on a device name or a profile name. After you enter the command, the switch is in the configure-macro-trigger mode and the **device**, **exit**, **no**, and **profile** keywords are visible. In this mode, you can provide a device name or a profile name to map to the trigger. It is not necessary to map the trigger to both a device name and a profile name. If you map the trigger to both names, the trigger-to-profile name mapping has preference for macro application.

You must use this command to configure a trigger when you configure a user-defined macro. The trigger name is required for the custom macro configuration.

After the device is profiled, you must add the complete string to the device-group database.

Example

This example shows how to configure a user-defined trigger for a profile called DMP_EVENT mediaplayer for use with a media player that has no built-in trigger:

```
Device(config)# macro auto trigger DMP
Device(config-macro-trigger)# profile mediaplayer-DMP
Device(config-macro-trigger)# exit
```

macro description

To enter a description about which macros are applied to an interface, use the **macro description** command in interface configuration mode. Use the **no** form of this command to remove the description. This command is mandatory for Auto SmartPorts to work.

macro description *text*
no macro description *text*

Syntax Description

description *text*	Enters a description about the macros that are applied to the specified interface.

Command Default

This command has no default setting.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Use the **description** keyword to associate comment text or the macro name with an interface. When multiple macros are applied on a single interface, the description text is from the last applied macro.

You can verify your settings by entering the **show parser macro description** command in privileged EXEC mode.

Example

This example shows how to add a description to an interface:

```
(config-if)# macro description duplex settings
```

macro global

To apply a macro to a switch or to apply and debug a macro on a switch, use the **macro global** command in global configuration mode.

macro global {**apply** | **trace**} *macro-name* [**parameter** {*value*}][**parameter** {*value*}][**parameter** {*value*}] parameter

Syntax Description

apply	Applies a macro to the switch.
trace	Applies a macro to a switch and debugs the macro.
macro-name	Specifies the name of the macro.
parameter *value*	(Optional) Specifies unique parameter values that are specific to the switch. You can enter up to three keyword-value pairs. Parameter keyword matching is case sensitive. All matching occurrences of the keyword are replaced with the corresponding value.

Command Default

This command has no default setting.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Note You can delete a global macro-applied configuration on a switch only by entering the no version of each command in the macro.

Use the **macro global apply** *macro-name* command to apply the macro to an interface.

Use the **macro global trace** *macro-name* command to apply and then debug the macro to find any syntax or configuration errors.

If a command fails when you apply a macro because of a syntax error or a configuration error, the macro continues to apply the remaining commands to the switch.

When creating a macro that requires the assignment of unique values, use the **parameter** *value* keywords to designate values specific to the switch.

Keyword matching is case sensitive. All matching occurrences of the keyword are replaced with the corresponding value. Any full match of a keyword, even if it is part of a larger string, is considered a match and is replaced by the corresponding value.

Some macros might contain keywords that require a parameter value. You can use the **macro global apply** *macro-name* ? command to display a list of any required values in the macro. If you apply a macro without entering the keyword values, the commands are invalid and are not applied.

There are Cisco-default Smartports macros embedded in the switch software. You can display these macros and the commands they contain by using the **show parser macro** command in user EXEC mode.

Follow these guidelines when you apply a Cisco-default Smartports macro on a switch:

- Display all macros on the switch by using the **show parser macro** command. Display the contents of a specific macro by using the **show parser macro name** *macro-name* command.
- Keywords that begin with $ mean that a unique parameter value is required. Append the Cisco-default macro with the required values by using the **parameter** *value* keywords.

  The Cisco-default macros use the $ character to help identify required keywords. There is no restriction on using the $ character to define keywords when you create a macro.

When you apply a macro to a switch, the macro name is automatically added to the switch. You can display the applied commands and macro names by using the **show running-config** command.

Example

After you have created a new macro by using the **macro auto execute** command, you can apply it to a switch. This example shows how to view the **snmp** macro, how to apply the macro, set the hostname to test-server, and set the IP precedence value to 7:

```
Device# show parser macro name snmp
Macro name : snmp
Macro type : customizable

#enable port security, linkup, and linkdown traps
snmp-server enable traps port-security
snmp-server enable traps linkup
snmp-server enable traps linkdown
#set snmp-server host
snmp-server host ADDRESS
#set SNMP trap notifications precedence
snmp-server ip precedence VALUE

----------------------------------------------------
Device(config)# macro global apply snmp ADDRESS test-server VALUE 7
```

To debug a macro, use the **macro global trace** command to find any syntax or configuration errors in the macro when you apply it to a switch. In this example, the **ADDRESS** parameter value was not entered, the **snmp-server host** command failed, and the remainder of the macro is applied to the switch:

```
Device(config)# macro global trace snmp VALUE 7
Applying command...'snmp-server enable traps port-security'
Applying command...'snmp-server enable traps linkup'
Applying command...'snmp-server enable traps linkdown'
Applying command...'snmp-server host'
%Error Unknown error.
Applying command...'snmp-server ip precedence 7'
```

macro global description

To enter a description about the macros that are applied to a switch, use the **macro global description** command in global configuration mode. Use the **no** form of this command to remove the description.

macro global description *text*

no macro global description *text*

Syntax Description

description *text*	Enters a description about the macros that are applied to the switch.

Command Default

This command has no default setting.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Use the **description** keyword to associate comment text or the macro name with a switch. When multiple macros are applied on a switch, the description text is from the last applied macro.

You can verify your settings by entering the **show parser macro description** command in privileged EXEC mode.

Example

This example shows how to add a description to a switch:

```
Device(config)# macro global description udld aggressive mode enabled
```

max-endpoints (coap-proxy configuration)

To specify the maximum number of endpoints that can be learnt on the device, use the **max-endpoints** command in coap-proxy configuration mode. To return to the default settings, use the **no** form of the command.

max-endpoints *number*
no max-endpoints

Syntax Description

number	Range is from 1 to 500

Command Default

The default number of endpoints is 10.

Command Modes

coap-proxy configuration (config-coap-proxy)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

To access coap-proxy configuration mode, enter the **coap proxy** command in global configuration mode.

Example

This example shows how to specify maximum endpoints as 12 that can be learnt on the device.

```
Device(config)# coap proxy
Device(config-coap-proxy)# max-endpoints 12
```

mdix auto

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

mdix auto
no mdix auto

Syntax Description

This command has no arguments or keywords.

Command Default

Auto-MDIX is enabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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

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

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

Auto-MDIX is supported on all 10/100 and 10/100/1000 Mb/s interfaces and on 10/100/1000BASE-TX small form-factor pluggable (SFP) module interfaces. It is not supported on 1000BASE-SX or -LX SFP module interfaces.

You can verify the operational state of auto-MDIX on the interface by entering the **show controllers ethernet-controller** *interface-id* **phy** privileged EXEC command.

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

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

network-policy

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

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

Syntax Description

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

Command Default

No network-policy profiles are applied.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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

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

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

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

network-policy profile (global configuration)

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

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

Syntax Description

profile-number	Network-policy profile number. The range is 1 to 4294967295.

Command Default

No network-policy profiles are defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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

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

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

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

This example shows how to create network-policy profile 60:

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

port-dtls (coap-proxy configuration)

To configure a Datagram Transport Layer Security (DTLS) port, use the **port-dtls** command in coap-proxy configuration mode. To return to the default settings, use the **no** form of the command.

port-dtls *number*
no port-dtls

Syntax Description

number	Range is from 1 to 65000.

Command Default

The default port is 5683.

Command Modes

coap-proxy configuration (config-coap-proxy)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

To access coap-proxy configuration mode, enter the **coap proxy** command in global configuration mode.

Example

This example shows how to configure a dtls port .

```
Device(config)# coap proxy
Device(config-coap-proxy)# port-dtls 5899
```

port-unsecure (coap-proxy configuration)

To configure a port, use the **port-unsecure** command in coap-proxy configuration mode. To return to the default settings, use the **no** form of the command.

port-unsecure *number*
no port-dtls

Syntax Description

number	Range is from 1 to 65000.

Command Default

The default port is 5683.

Command Modes

coap-proxy configuration (config-coap-proxy)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

To access coap-proxy configuration mode, enter the **coap proxy** command in global configuration mode.

Example

This example shows how to configure a port .

```
Device(config)# coap proxy
Device(config-coap-proxy)# port-unsecure 5899
```

power inline

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

power inline {**auto** [**max** *max-wattage*] | **never** | **port priority** {**high** | **low**} | **static** [**max** *max-wattage*]}
no power inline {**auto** | **never** | **port priority** {**high** | **low**} | **static** [**max** *max-wattage*]}

Syntax Description

auto	Enables powered-device detection. If enough power is available, automatically allocates power to the PoE port after device detection. Allocation is first-come, first-serve.
max *max-wattage*	(Optional) Limits the power allowed on the port. The range is 4000 to 30000 mW. If no value is specified, the maximum is allowed.
never	Disables device detection, and disables power to the port.
port	Configures the power priority of the port. The default priority is low.
priority {**high** | **low**}	Sets the power priority of the port. In case of a power supply failure, ports configured as low priority are turned off first and ports configured as high priority are turned off last. The default priority is low.
static	Enables powered-device detection. Pre-allocates (reserves) power for a port before the switch discovers the powered device. This action guarantees that the device connected to the interface receives enough power.

Command Default

The default is **auto** (enabled).

The maximum wattage is 30,000 mW.

The default port priority is low.

Command Default

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

This command is supported only on PoE-capable ports. If you enter this command on a port that does not support PoE, this error message appears:

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

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

Use the **max** *max-wattage* option to disallow higher-power powered devices. With this configuration, when the powered device sends Cisco Discovery Protocol (CDP) messages requesting more power than the maximum wattage, the switch removes power from the port. If the powered-device IEEE class maximum is greater than the maximum wattage, the switch does not power the device. The power is reclaimed into the global power budget.

Note The switch never powers any class 0 or class 3 device if the **power inline max max-wattage** command is configured for less than 30 W.

If the switch denies power to a powered device (the powered device requests more power through CDP messages or if the IEEE class maximum is greater than the maximum wattage), the PoE port is in a power-deny state. The switch generates a system message, and the Oper column in the **show power inline** privileged EXEC command output shows *power-deny*.

Use the **power inline static max** *max-wattage* command to give a port high priority. The switch allocates PoE to a port configured in static mode before allocating power to a port configured in auto mode. The switch reserves power for the static port when it is configured rather than upon device discovery. The switch reserves the power on a static port even when there is no connected device and whether or not the port is in a shutdown or in a no shutdown state. The switch allocates the configured maximum wattage to the port, and the amount is never adjusted through the IEEE class or by CDP messages from the powered device. Because power is pre-allocated, any powered device that uses less than or equal to the maximum wattage is guaranteed power when it is connected to a static port. However, if the powered device IEEE class is greater than the maximum wattage, the switch does not supply power to it. If the switch learns through CDP messages that the powered device needs more than the maximum wattage, the powered device is shut down.

If the switch cannot pre-allocate power when a port is in static mode (for example, because the entire power budget is already allocated to other auto or static ports), this message appears: Command rejected: power inline static: pwr not available. The port configuration remains unchanged.

When you configure a port by using the **power inline auto** or the **power inline static** interface configuration command, the port autonegotiates by using the configured speed and duplex settings. This is necessary to determine the power requirements of the connected device (whether or not it is a powered device). After the power requirements have been determined, the switch hardcodes the interface by using the configured speed and duplex settings without resetting the interface.

When you configure a port by using the **power inline never** command, the port reverts to the configured speed and duplex settings.

If a port has a Cisco powered device connected to it, you should not use the **power inline never** command to configure the port. A false link-up can occur, placing the port in an error-disabled state.

Use the **power inline port priority {high | low}** command to configure the power priority of a PoE port. Powered devices connected to ports with low port priority are shut down first in case of a power shortage.

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

Examples

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

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

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

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

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

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

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

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# power inline port priority high
```

power inline police

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

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

Syntax Description

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

Command Default

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

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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

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

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

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

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

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

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

an *Icut* fault for drawing more current than the maximum. The port remains in the fault state for a time before attempting to power on again. If the port continuously draws more than 15.4 W, the cycle repeats.

When a powered device connected to a PoE+ port restarts and sends a CDP or LLDP packet with a power TLV, the device locks to the power-negotiation protocol of that first packet and does not respond to power requests from the other protocol. For example, if the device is locked to CDP, it does not provide power to devices that send LLDP requests. If CDP is disabled after the device has locked on it, the device does not respond to LLDP power requests and can no longer power on any accessories. In this case, you should restart the powered device.

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

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

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

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

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

Examples

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

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

power supply

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

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

Syntax Description

stack-member-number	Stack member number for which to configure the internal power supplies. The range is 1 to 9, depending on the number of switches in the stack. This parameter is available only on stacking-capable switches.
slot	Selects the switch power supply to set.
A	Selects the power supply in slot A.
B	Selects the power supply in slot B. **Note** Power supply slot B is the closest slot to the outer edge of the switch.
off	Sets the switch power supply to off.
on	Sets the switch power supply to on.

Command Default

The switch power supply is on.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The **power supply** command applies to a switch or to a switch stack where all switches are the same platform.

In a switch stack with the same platform switches, you must specify the stack member before entering the **slot** {**A** | **B**} **off** or **on** keywords.

To return to the default setting, use the **power supply** *stack-member-number* **on** command.

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

Examples

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

```
Device> power supply 2 slot A off
Disabling Power supply A may result in a power loss to PoE devices and/or switches ...
Continue? (yes/[no]): yes
Device
Jun 10 04:52:54.389: %PLATFORM_ENV-6-FRU_PS_OIR: FRU Power Supply 1 powered off
Jun 10 04:52:56.717: %PLATFORM_ENV-1-FAN_NOT_PRESENT: Fan is not present
```

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

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

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

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

resource directory (coap-proxy configuration)

To unicast upstream resource directory server to which the switch can act as a COAP client, use the **resource directory** command in coap-proxy configuration mode. To return to the default settings, use the **no** form of the command.

A maximum of five ip-lists can be configured, for each ipv4 or ipv6, using the resource directory command.

resource directory {**ipv4** | **ipv6**}[*ip-address*]
no resource directory

Syntax Description

ipv4 *ip-address*	Specifies IPv4 address.
ipv6 *ip-address*	Specifies IPv6 address.

Command Modes

coap-proxy configuration (config-coap-proxy)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

To access coap-proxy configuration mode, enter the **coap proxy** command in global configuration mode.

Example

This example shows how to unicast upstream resource directory server to which the switch can act as a COAP client.

```
Device(config)# coap proxy
Device(config-coap-proxy)# resource-directory ipv4 192.168.1.1
```

security (coap-proxy configuration)

To configure CoAP security features, use the **security** command in coap-proxy configuration mode. To return to the default settings, use the **no** form of the command.

security {**none** [{**ipv4** { *ip-address ip-mask/prefix*} | **ipv6**{ *ip-address ip-mask/prefix*} | **list**{*ipv4-list-name ipv6-list-name*}}] | **dtls** {[**id-trustpoint** {*identity-trustpoint label*}][**verification-trustpoint** { *verification-trustpoint*}] | [{**ipv4** { *ip-address ip-mask/prefix*} | **ipv6**{ *ip-address ip-mask/prefix*} | **list**{*ipv4-list-name ipv6-list-name*}}]}}
no security

Syntax Description

none	Indicates no security on that port. **Note** A maximum of five ipv4 and five ipv6 addresses can be associated.
dtls	The DTLS security takes RSA trustpoint and Verification trustpoint which are optional. Without 1.1.0.0 255.255.0.0 Verification trustpoint it does the normal Public Key Exchange. **Note** A maximum of five ipv4 and five ipv6 addresses can be associated.

Command Modes

coap-proxy configuration (config-coap-proxy)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

To access coap-proxy configuration mode, enter the **coap proxy** command in global configuration mode.

Example

This example shows how to configure no security on the port.

```
Device(config)# coap proxy
Device(config-coap-proxy)# security none ipv4 1.1.0.0 255.255.0.0
```

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*

Syntax Description

identifier	Specifies the event trigger identifier. The identifier should have no spaces or hyphens between words.
description	Specifies the event trigger description text.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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

rp {**active**	**standby**}	Specifies the active or the standby Switch whose beacon LED status is to be displayed.
slot *slot-num*	Specifies the slot whose beacon LED status is to be displayed.
all	Displays the status of all beacon LEDs.

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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 coap dtls endpoints

To display the CoAP dtls endpoints, use the **show coap dtls endpoints** command in user EXEC or privileged EXEC mode.

show coap dtls endpoints

Command Default This command has no arguments or keywords.

Command Modes User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Example

This example shows how to display the CoAP dtls endpoint:

```
Device# show coap dtls endpoints
#     Index StateString StateValue  Port IP
------------------------------------------------------------------
```

show coap endpoints

To display the CoAP endpoints, use the **show coap endpoints** command in user EXEC or privileged EXEC mode.

show coap endpoints

Command Default

This command has no arguments or keywords.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Example

This example shows how to display the CoAP endpoint

```
Device# show coap endpoints
List of all endpoints :

Code : D - Discovered , N - New
#    Status  Age(s)    LastWKC(s)    IP
---------------------------------------------------------------

Endpoints - Total : 0 Discovered : 0 New : 0
```

show coap globals

To display the CoAP globals, use the **show coap globals** command in user EXEC or privileged EXEC mode.

show coap globals

Command Default

This command has no arguments or keywords.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Example

The following is sample output from the **show coap globals** command:

This example shows how to display the CoAP configuration:

```
Device# show coap dtls globals
Coap System Timer Values :
 Discovery  : 120 sec
 Cache Exp  : 5 sec
 Keep Alive : 120 sec
 Client DB  : 5 sec
 Query Queue: 500 ms
 Ack delay  : 500 ms
 Timeout    : 5 sec
 Ageout     : 300 sec

Max Endpoints      : 10

Max DTLS Endpoints : 20
Resource Disc Mode : POST
```

show coap resources

To display the CoAP resources, use the **show coap resources** command in user EXEC or privileged EXEC mode.

show coap resources

Command Default

This command has no arguments or keywords.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Example

This example shows how to display the CoAP resources:

```
Device# show coap resources
Link format data =

</>
</cisco/flood>
</cisco/context>
</cisco/showtech>
</cisco/discover>
</cisco/sleep>
</cisco/lldp>
```

show coap stats

To display the CoAP stats, use the **show coap stats** command in user EXEC or privileged EXEC mode.

show coap stats

Command Default

This command has no arguments or keywords.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Example

This example shows how to display the CoAP stats:

```
Device# show coap stats
Coap Stats :
Endpoints    : 0
Requests     : 20
Ext Queries  : 0
New Endpoints: 0
```

show coap version

To display the CoAP version, use the **show coap version** command in user EXEC or privileged EXEC mode.

show coap version

Command Default

This command has no arguments or keywords.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Example

This example shows how to display the CoAP version:

```
Device# show coap version
CoAP version 1.0.5
RFC 7252
```

show device classifier attached

To display the devices connected to a switch and their associated properties, use the **show device classifier attached** command in user EXEC mode.

show device classifier attached [{**detail** | **interface** *interface_id* | **mac-address** *mac_address*}]

Syntax Description

detail	Displays detailed device classifier information.
interface *interface_id*	Displays information about devices attached to the specified interface.
mac *mac_address*	Displays device information for the specified endpoint.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Use this command to display the devices connected to a switch. Use the **show device classifier attached** command in privileged EXEC mode to display the configurable parameters for a device.

Example

This example shows how to use the **show device classifier attached** command with no optional keywords to view the devices connected to the switch:

```
Device# show device classifier attached
MAC_Address       Port_Id     Profile Name
==============    =======     ============================
000a.b8c6.1e07    Gi1/0/2    Cisco-Device
001f.9e90.1250    Gi1/0/4    Cisco-AP-Aironet-1130
=====================================================
```

This example shows how to use the **show device classifier attached** command in privileged EXEC mode with the optional **mac-address** keyword to view summary information about the connected device with the specified MAC address:

```
Device# show device classifier attached mac-address 001f.9e90.1250
MAC_Address       Port_Id     Profile Name
==============    =======     ============================
001f.9e90.1250    Gi1/0/4    Cisco-AP-Aironet-1130
=========================================================
```

This example shows how to use the **show device classifier attached** command in privileged EXEC mode with the optional **mac-address** and **detail** keywords to view detailed information about the connected device with the specified MAC address:

```
Device# show device classifier attached mac-address 001f.9e90.1250 detail
MAC_Address       Port_Id     Certainty Parent    ProfileType      Profile Name
     Device_Name
==============    =======     ========= ======    ===========  ============================
    ===========
001f.9e90.1250    Gi1/0/4      40       2         Built-in       Cisco-AP-Aironet-1130
    cisco AIR-LAP1131AG-E-K9
=================================================================================================
```

This example shows how to use the **show device classifier attached** command in privileged EXEC mode with the optional **interface** keyword to view summary information about the device connected to the specified interface:

```
Device# show device classifier attached interface gi 1/0/2
MAC_Address       Port_Id          Profile Name
==============    =======     ============================
000a.b8c6.1e07    Gi1/0/2    Cisco-Device
=====================================================
```

This example shows how to use the **show device classifier attached** command in privileged EXEC mode with the optional **interface** and **detail** keywords to view detailed information about the device connected to the specified interface:

```
Device# show device classifier attached interface gi 1/0/2 detail
MAC_Address       Port_Id     Certainty Parent    ProfileType  Profile Name
     Device_Name
==============    =======     ========= ======    ===========  ============================
    ===========
000a.b8c6.1e07    Gi1/0/2      10       0        Default       Cisco-Device        cisco
WS-C2960-48TT-L
=================================================================================================
```

show device classifier clients

To display the clients using the device classifier facility on the switch, use the **show device classifier clients** command in user EXEC mode.

show device classifier clients

Command Default

This command has no arguments or keywords.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Device classifier (DC) is enabled by default when you enable a client application (for example, Auto SmartPorts) that uses its functionality. Use the **show device classifier clients** command to display the clients that are using the DC feature on the switch.

As long as any clients are using the DC, you cannot disable it by using the **no device classifier** command. If you attempt to disable the DC while a client is using it, an error message appears.

Example

This example shows how to use the **show device classifier clients** command to view the clients using the DC on the switch:

```
Device# show device classifier clients
Client Name
====================
Auto Smart Ports

This example shows the error message that appears when you attempt to disable DC while a
client is using it:
Switch(config)# no device classifier
These subsystems should be disabled before disabling Device classifier
Auto Smart Ports

% Error - device classifier is not disabled
```

show device classifier profile type

To display all the device types recognized by the device classifier, use the **show device classifier profile type** command in user EXEC mode.

show device classifier profile type [{**table** [{*built-in default*}] | **string** *filter_string*}]

Syntax Description

table	Displays device classification in a table.
built-in	Displays device classification information from the built-in device table.
default	Displays device classification information from the default device table.
filter *string*	Displays information for devices that match the filter.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

This command displays all the device types recognized by the device classification engine. The number of available device types is the number of profiles stored on the switch. Because the number of profiles can be very large, you can use the **filter** keyword to limit the command output.

Example

This example shows how to use the **show device classifier profile type** command in privileged EXEC mode with no optional keywords to view the devices recognized by the device classifier:

```
Device# show device classifier profile type table
  Valid         Type       Profile Name                          min Conf   ID
==========  =========  ==================                        ========  ====
  Valid        Default      Apple-Device                             10        0
  Valid        Default      Aruba-Device                             10        1
  Valid        Default      Avaya-Device                             10        2
  Valid        Default      Avaya-IP-Phone                           20        3
  Valid        Default      BlackBerry                               20        4
  Valid        Default      Cisco-Device                             10        5
  Valid        Default      Cisco-IP-Phone                           20        6
  Valid        Default      Cisco-IP-Phone-7902                      70        7
  Valid        Default      Cisco-IP-Phone-7905                      70        8
  Valid        Default      Cisco-IP-Phone-7906                      70        9
  Valid        Default      Cisco-IP-Phone-7910                      70        10
  Valid        Default      Cisco-IP-Phone-7911                      70        11
  Valid        Default      Cisco-IP-Phone-7912                      70        12
  Valid        Default      Cisco-IP-Phone-7940                      70        13
  Valid        Default      Cisco-IP-Phone-7941                      70        14
  Valid        Default      Cisco-IP-Phone-7942                      70        15
```

```
Valid        Default      Cisco-IP-Phone-7945                    70        16
Valid        Default      Cisco-IP-Phone-7945G                   70        17
Valid        Default      Cisco-IP-Phone-7960                    70        18
Valid        Default      Cisco-IP-Phone-7961                    70        19
Valid        Default      Cisco-IP-Phone-7962                    70        20
Valid        Default      Cisco-IP-Phone-7965                    70        21
Valid        Default      Cisco-IP-Phone-7970                    70        22
Valid        Default      Cisco-IP-Phone-7971                    70        23
Valid        Default      Cisco-IP-Phone-7975                    70        24
Valid        Default      Cisco-IP-Phone-7985                    70        25
Valid        Default      Cisco-IP-Phone-9971                    70        26
Valid        Default      Cisco-WLC-2100-Series                  40        27
Valid        Default      DLink-Device                           10        28
Valid        Default      Enterasys-Device                       10        29
Valid        Default      HP-Device                              10        30
Valid        Default      HP-JetDirect-Printer                   30        31
Valid        Default      Lexmark-Device                         10        32
Valid        Default      Lexmark-Printer-E260dn                 30        33
Valid        Default      Microsoft-Device                       10        34
Valid        Default      Netgear-Device                         10        35
Valid        Default      NintendoWII                            10        36
Valid        Default      Nortel-Device                          10        37
Valid        Default      Nortel-IP-Phone-2000-Series            20        38
Valid        Default      SonyPS3                                10        39
Valid        Default      XBOX360                                20        40
Valid        Default      Xerox-Device                           10        41
Valid        Default      Xerox-Printer-Phaser3250               30        42
Valid        Default      Aruba-AP                               20        43
Valid        Default      Cisco-Access-Point                     10        44
Valid        Default      Cisco-IP-Conference-Station-7935       70        45
Valid        Default      Cisco-IP-Conference-Station-7936       70        46
Valid        Default      Cisco-IP-Conference-Station-7937       70        47
Valid        Default      DLink-DAP-1522                         20        48
Valid        Default      Cisco-AP-Aironet-1130                  30        49
Valid        Default      Cisco-AP-Aironet-1240                  30        50
Valid        Default      Cisco-AP-Aironet-1250                  30        51
Valid        Default      Cisco-AIR-LAP                          25        52
Valid        Default      Cisco-AIR-LAP-1130                     30        53
Valid        Default      Cisco-AIR-LAP-1240                     50        54
Valid        Default      Cisco-AIR-LAP-1250                     50        55
Valid        Default      Cisco-AIR-AP                           25        56
Valid        Default      Cisco-AIR-AP-1130                      30        57
Valid        Default      Cisco-AIR-AP-1240                      50        58
Valid        Default      Cisco-AIR-AP-1250                      50        59
Invalid      Default      Sun-Workstation                        10        60
Valid        Default      Linksys-Device                         20        61
Valid        Default      LinksysWAP54G-Device                   30        62
Valid        Default      HTC-Device                             10        63
Valid        Default      MotorolaMobile-Device                  10        64
Valid        Default      VMWare-Device                          10        65
Valid        Default      ISE-Appliance                          10        66
Valid        Built-in     Cisco-Device                           10        0
Valid        Built-in     Cisco-Router                           10        1
Valid        Built-in     Router                                 10        2
Valid        Built-in     Cisco-IP-Camera                        10        3
Valid        Built-in     Cisco-IP-Camera-2xxx                   30        4
Valid        Built-in     Cisco-IP-Camera-2421                   50        5
Valid        Built-in     Cisco-IP-Camera-2500                   50        6
Valid        Built-in     Cisco-IP-Camera-2520                   50        7
Valid        Built-in     Cisco-IP-Camera-2530                   50        8
Valid        Built-in     Cisco-IP-Camera-4xxx                   50        9
Valid        Built-in     Cisco-Transparent-Bridge               8         10
Valid        Built-in     Transparent-Bridge                     8         11
Valid        Built-in     Cisco-Source-Bridge                    10        12
```

```
Valid        Built-in     Cisco-Switch                    10        13
Valid        Built-in     Cisco-IP-Phone                  20        14
Valid        Built-in     IP-Phone                        20        15
Valid        Built-in     Cisco-DMP                       10        16
Valid        Built-in     Cisco-DMP-4305G                 70        17
Valid        Built-in     Cisco-DMP-4310G                 70        18
Valid        Built-in     Cisco-DMP-4400G                 70        19
Valid        Built-in     Cisco-WLC-2100-Series           40        20
Valid        Built-in     Cisco-Access-Point              10        21
Valid        Built-in     Cisco-AIR-LAP                   30        22
Valid        Built-in     Cisco-AIR-AP                    30        23
Valid        Built-in     Linksys-Device                  20        24
```

show environment

To display fan, temperature, and power information, use the **show environment** command in EXEC mode.

show environment { **all** | **fan** | **power** | **stack** | **temperature** }

Syntax Description

all	Displays the fan and temperature environmental status and the status of the internal power supplies.
fan	Displays the switch fan status.
power	Displays the internal power status of the active switch.
stack	Displays all environmental status for each switch in the stack or for the specified switch. This keyword is available only on stacking-capable switches.
temperature	Displays the switch temperature status.

Command Default

None

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Use the **show environment** EXEC command to display the information for the switch being accessed—a standalone switch or the active switch. Use this command with the **stack** keyword to display all information for the stack or for the specified stack member.

If you enter the **show environment temperature status** command, the command output shows the switch temperature state and the threshold level.

You can also use the **show environment 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*.

Examples

This example shows a sample output of the **show environment all** command:

```
Device> show environment 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
```

This example shows a sample output of the **show environment power** command:

```
Device> show environment 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
```

This example shows a sample output of the **show environment stack** command:

```
Device# show environment stack

System Temperature Value: 41 Degree Celsius
System Temperature State: GREEN
Yellow Threshold : 66 Degree Celsius
Red Threshold    : 76 Degree Celsius
```

This example shows a sample output of the **show environment temperature** command:

```
Device> show environment 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 14: States in the show environment temperature status Command Output

State	Description
Green	The switch temperature is in the *normal* operating range.
Yellow	The temperature is in the *warning* range. You should check the external temperature around the switch.
Red	The temperature is in the *critical* range. The switch might not run properly if the temperature is in this range.

show errdisable detect

To display error-disabled detection status, use the **show errdisable detect** command in EXEC mode.

show errdisable detect

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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

The error-disable reasons in the command output are listed in alphabetical order. The mode column shows how error-disable is configured for each feature.

You can configure error-disabled detection in these modes:

- port mode—The entire physical port is error-disabled if a violation occurs.
- vlan mode—The VLAN is error-disabled if a violation occurs.
- port/vlan mode—The entire physical port is error-disabled on some ports and is per-VLAN error-disabled on other ports.

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

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

```
udld                Enabled      port
vmps                Enabled      port
```

show errdisable recovery

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

show errdisable recovery

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	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 ip interface

To display the usability status of interfaces configured for IP, use the **show ip interface** command in privileged EXEC mode.

show ip interface [*type number*] [**brief**]

Syntax Description

type	(Optional) Interface type.
number	(Optional) Interface number.
brief	(Optional) Displays a summary of the usability status information for each interface. **Note** The output of the **show ip interface brief** command displays information of all the available interfaces whether or not the corresponding network module for these interfaces are connected. These interfaces can be configured if the network module is connected. Run the **show interface status** command to see which network modules are connected.

Command Default

The full usability status is displayed for all interfaces configured for IP.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The Cisco IOS software automatically enters a directly connected route in the routing table if the interface is usable (which means that it can send and receive packets). If an interface is not usable, the directly connected routing entry is removed from the routing table. Removing the entry lets the software use dynamic routing protocols to determine backup routes to the network, if any.

If the interface can provide two-way communication, the line protocol is marked "up." If the interface hardware is usable, the interface is marked "up."

If you specify an optional interface type, information for that specific interface is displayed. If you specify no optional arguments, information on all the interfaces is displayed.

When an asynchronous interface is encapsulated with PPP or Serial Line Internet Protocol (SLIP), IP fast switching is enabled. A **show ip interface** command on an asynchronous interface encapsulated with PPP or SLIP displays a message indicating that IP fast switching is enabled.

You can use the **show ip interface brief** command to display a summary of the device interfaces. This command displays the IP address, the interface status, and other information.

The **show ip interface brief** command does not display any information related to Unicast RPF.

Examples

The following example shows interface information on Gigabit Ethernet interface 1/0/1:

```
Device# show ip interface gigabitethernet 1/0/1
```

```
GigabitEthernet1/0/1 is up, line protocol is up
  Internet address is 10.1.1.1/16
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP Feature Fast switching turbo vector
  IP VPN Flow CEF switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Policy routing is enabled, using route map PBR
  Network address translation is disabled
  BGP Policy Mapping is disabled
  IP Multi-Processor Forwarding is enabled
     IP Input features, "PBR",
         are not supported by MPF and are IGNORED
     IP Output features, "NetFlow",
         are not supported by MPF and are IGNORED
```

The following example shows how to display the usability status for a specific VLAN:

```
Device# show ip interface vlan 1

Vlan1 is up, line protocol is up
  Internet address is 10.0.0.4/24
  Broadcast address is 255.255.255.255
Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is enabled
```

```
IP Fast switching turbo vector
IP Normal CEF switching turbo vector
IP multicast fast switching is enabled
IP multicast distributed fast switching is disabled
IP route-cache flags are Fast, CEF
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Probe proxy name replies are disabled
Policy routing is disabled
Network address translation is disabled
WCCP Redirect outbound is disabled
WCCP Redirect inbound is disabled
WCCP Redirect exclude is disabled
BGP Policy Mapping is disabled
Sampled Netflow is disabled
IP multicast multilayer switching is disabled
Netflow Data Export (hardware) is enabled
```

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

Table 15: show ip interface Field Descriptions

Field	Description
Broadcast address is	Broadcast address.
Peer address is	Peer address.
MTU is	MTU value set on the interface, in bytes.
Helper address	Helper address, if one is set.
Directed broadcast forwarding	Shows whether directed broadcast forwarding is enabled.
Outgoing access list	Shows whether the interface has an outgoing access list set.
Inbound access list	Shows whether the interface has an incoming access list set.
Proxy ARP	Shows whether Proxy Address Resolution Protocol (ARP) is enabled for the interface.
Security level	IP Security Option (IPSO) security level set for this interface.
Split horizon	Shows whether split horizon is enabled.
ICMP redirects	Shows whether redirect messages will be sent on this interface.
ICMP unreachables	Shows whether unreachable messages will be sent on this interface.
ICMP mask replies	Shows whether mask replies will be sent on this interface.
IP fast switching	Shows whether fast switching is enabled for this interface. It is generally enabled on serial interfaces, such as this one.
IP Flow switching	Shows whether Flow switching is enabled for this interface.

Field	Description
IP CEF switching	Shows whether Cisco Express Forwarding switching is enabled for the interface.
IP multicast fast switching	Shows whether multicast fast switching is enabled for the interface.
IP route-cache flags are Fast	Shows whether NetFlow is enabled on an interface. Displays "Flow init" to specify that NetFlow is enabled on the interface. Displays "Ingress Flow" to specify that NetFlow is enabled on a subinterface using the **ip flow ingress**command. Shows "Flow" to specify that NetFlow is enabled on a main interface using the **ip route-cache flow** command.
Router Discovery	Shows whether the discovery process is enabled for this interface. It is generally disabled on serial interfaces.
IP output packet accounting	Shows whether IP accounting is enabled for this interface and what the threshold (maximum number of entries) is.
TCP/IP header compression	Shows whether compression is enabled.
WCCP Redirect outbound is disabled	Shows the status of whether packets received on an interface are redirected to a cache engine. Displays "enabled" or "disabled."
WCCP Redirect exclude is disabled	Shows the status of whether packets targeted for an interface will be excluded from being redirected to a cache engine. Displays "enabled" or "disabled."
Netflow Data Export (hardware) is enabled	NetFlow Data Expert (NDE) hardware flow status on the interface.

The following example shows how to display a summary of the usability status information for each interface:

```
Device# show ip interface brief

Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  unassigned      YES NVRAM  administratively down down
GigabitEthernet0/0     unassigned      YES NVRAM  down                  down
GigabitEthernet1/0/1   unassigned      YES NVRAM  down                  down
GigabitEthernet1/0/2   unassigned      YES unset  down                  down
GigabitEthernet1/0/3   unassigned      YES unset  down                  down
GigabitEthernet1/0/4   unassigned      YES unset  down                  down
GigabitEthernet1/0/5   unassigned      YES unset  down                  down
GigabitEthernet1/0/6   unassigned      YES unset  down                  down
GigabitEthernet1/0/7   unassigned      YES unset  down                  down

<output truncated>
```

Table 16: show ip interface brief Field Descriptions

Field	Description
Interface	Type of interface.

Field	Description
IP-Address	IP address assigned to the interface.
OK?	"Yes" means that the IP Address is valid. "No" means that the IP Address is not valid.
Method	The Method field has the following possible values: • RARP or SLARP: Reverse Address Resolution Protocol (RARP) or Serial Line Address Resolution Protocol (SLARP) request. • BOOTP: Bootstrap protocol. • TFTP: Configuration file obtained from the TFTP server. • manual: Manually changed by the command-line interface. • NVRAM: Configuration file in NVRAM. • IPCP: **ip address negotiated** command. • DHCP: **ip address dhcp** command. • unset: Unset. • other: Unknown.
Status	Shows the status of the interface. Valid values and their meanings are: • up: Interface is up. • down: Interface is down. • administratively down: Interface is administratively down.
Protocol	Shows the operational status of the routing protocol on this interface.

Related Commands

Command	Description
ip interface	Configures a virtual gateway IP interface on a Secure Socket Layer Virtual Private Network (SSL VPN) gateway
show interface status	Displays the status of the interface.

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*] | **description** | **etherchannel** | **flowcontrol** | **link** [**module** *number*] | **private-vlan mapping** | **pruning** | **stats** | **status** [{ **err-disabled** | **inactive** }] | **trunk** }]

Syntax Description

interface-id	(Optional) ID of the interface. Valid interfaces include physical ports (including type, stack member for stacking-capable switches, module, and port number) and port channels. The port channel range is 1 to 48.
vlan *vlan-id*	(Optional) VLAN identification. The range is 1 to 4094.
accounting	(Optional) Displays accounting information on the interface, including active protocols and input and output packets and octets. **Note** The display shows only packets processed in software; hardware-switched packets do not appear.
capabilities	(Optional) Displays the capabilities of all interfaces or the specified interface, including the features and options that you can configure on the interface. Though visible in the command line help, this option is not available for VLAN IDs.
module *number*	(Optional) Displays capabilities of all interfaces on the switch or specified stack member. This option is not available if you entered a specific interface ID.
description	(Optional) Displays the administrative status and description set for interfaces. **Note** The output of the **show interfaces description** command displays information of all the available interfaces whether or not the corresponding network module for these interfaces are connected. These interfaces can be configured if the network module is connected. Run the **show interface status** command to see which network modules are connected.
etherchannel	(Optional) Displays interface EtherChannel information.
flowcontrol	(Optional) Displays interface flow control information.
link [**module***number*]	(Optional) Displays the up time and down time of the interface.

private-vlan mapping	(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.
pruning	(Optional) Displays trunk VTP pruning information for the interface.
stats	(Optional) Displays the input and output packets by switching the path for the interface.
status	(Optional) Displays the status of the interface. A status of unsupported in the Type field means that a non-Cisco small form-factor pluggable (SFP) module is inserted in the module slot.
err-disabled	(Optional) Displays interfaces in an error-disabled state.
inactive	(Optional) Displays interfaces in an inactive state.
trunk	(Optional) Displays interface trunk information. If you do not specify an interface, only information for active trunking ports appears.

Note Though visible in the command-line help strings, the **crb**, **fair-queue**, **irb**, **mac-accounting**, **precedence**, **random-detect**, **rate-limit**, and **shape** keywords are not supported.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.
Cisco IOS XE Gibraltar 16.12.1	The **link** keyword was introduced.

Usage Guidelines

The **show interfaces capabilities** command with different keywords has these results:

- Use the **show interface capabilities module** *number* command to display the capabilities of all interfaces on that switch in the stack. If there is no switch with that module number in the stack, there is no output.
- Use the **show interfaces** *interface-id* **capabilities** to display the capabilities of the specified interface.
- Use the **show interfaces capabilities** (with no module number or interface ID) to display the capabilities of all interfaces in the stack.

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 useful for knowing when a dead interface failed.

The **show interfaces link** command with different keywords has these results:

- Use the **show interface link module** *number* command to display the up time and down time 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.

Note On a standalone switch, the **module** *number* refers to the slot number.

- Use the **show interfaces** *interface-id* **link** to display the up time and down time of the specified interface.
- Use the **show interfaces link** (with no module number or interface ID) to display the up time and down time of all interfaces in the stack.
- If the interface is up, the up time displays the time (hours, minutes, and seconds) and the down time displays 00:00:00.
- If the interface is down, only the down time displays the time (hours, minutes, and seconds).

Examples

This is an example of output from the **show interfaces** command for an interface on stack member 3:

```
Device# show interfaces gigabitethernet3/0/2

GigabitEthernet3/0/2 is down, line protocol is down (notconnect)
  Hardware is Gigabit Ethernet, address is 2037.064d.4381 (bia 2037.064d.4381)
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Auto-duplex, Auto-speed, media type is 10/100/1000BaseTX
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
```

```
     0 input packets with dribble condition detected
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out

Device# show interfaces 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
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
                   Other     165476   11417844          0          0
           Spanning Tree    1240284   64494768          0          0
                     ARP       7096     425760          0          0
                     CDP      41368   18781072      82908   35318808
GigabitEthernet1/0/1
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
No traffic sent or received on this interface.
GigabitEthernet1/0/2
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
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 gigabitethernet1/0/2 description

Interface                      Status         Protocol Description
Gi1/0/2                        up             down     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** *interface-id* **pruning** command when pruning is enabled in the VTP domain:

```
Device# show interfaces gigabitethernet1/0/2 pruning

Port      Vlans pruned for lack of request by neighbor
Gi1/0/2   3,4

Port      Vlans traffic requested of neighbor
```

```
Gi1/0/2   1-3
```

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

```
Device# show interfaces vlan 1 stats

Switching path    Pkts In    Chars In    Pkts Out    Chars Out
     Processor    1165354   136205310      570800     91731594
   Route cache          0           0           0            0
         Total    1165354   136205310      570800     91731594
```

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

```
Device# show interfaces status err-disabled

Port      Name       Status         Reason
Gi1/0/2              err-disabled   gbic-invalid
Gi2/0/3              err-disabled   dtp-flap
```

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

```
Device# show interfaces gigabitethernet1/0/2 pruning

Port Vlans pruned for lack of request by neighbor


Device# show interfaces gigabitethernet1/0/1 trunk

Port        Mode             Encapsulation  Status        Native vlan
Gi1/0/1     on               802.1q         other         10

Port        Vlans allowed on trunk
Gi1/0/1     none

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

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

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

```
Device# show interfaces description

Interface                      Status         Protocol Description
Vl1                            admin down     down
Gi0/0                          down           down
Gi1/0/1                        down           down
Gi1/0/2                        down           down
Gi1/0/3                        down           down
Gi1/0/4                        down           down
Gi1/0/5                        down           down
Gi1/0/6                        down           down
Gi1/0/7                        down           down

<output truncated>
```

The following is a sample output of the **show interfaces link** command:

```
Device> enable
Device# show interfaces link
Port           Name               Down Time      Up Time
Gi1/0/1                           6w0d
Gi1/0/2                           6w0d
Gi1/0/3                           00:00:00       5w3d
Gi1/0/4                           6w0d
Gi1/0/5                           6w0d
Gi1/0/6                           6w0d
Gi1/0/7                           6w0d
Gi1/0/8                           6w0d
Gi1/0/9                           6w0d
Gi1/0/10                          6w0d
Gi1/0/11                          2d17h
Gi1/0/12                          6w0d
Gi1/0/13                          6w0d
Gi1/0/14                          6w0d
Gi1/0/15                          6w0d
Gi1/0/16                          6w0d
Gi1/0/17                          6w0d
Gi1/0/18                          6w0d
Gi1/0/19                          6w0d
Gi1/0/20                          6w0d
Gi1/0/21                          6w0d
```

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. The range is 1 to 9. **Note** In this command, the **module** keyword refers to the stack member number. The module number that is part of the interface ID is always zero.
protocol status	(Optional) Displays the status of protocols enabled on interfaces.
trunk	(Optional) Displays trunk counters.

Note Though visible in the command-line help string, the **vlan** *vlan-id* keyword is not supported.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

If you do not enter any keywords, all counters for all interfaces are included.

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

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

```
<output truncated>
```

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

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

<output truncated>
```

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

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

<output truncated>
```

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

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

<output truncated>
```

show interfaces switchport

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

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

Syntax Description

interface-id	(Optional) ID of the interface. Valid interfaces include physical ports (including type, stack member for stacking-capable switches, module, and port number) and port channels. The port channel range is 1 to 48.
module *number*	(Optional) Displays switchport configuration of all interfaces on the switch or specified stack member. This option is not available if you entered a specific interface ID.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Use the **show interface switchport module** *number* command to display the switch port characteristics of all interfaces on that switch in the stack. If there is no switch with that module number in the stack, there is no output.

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

```
Device# show interfaces gigabitethernet1/0/1 switchport
Name: Gi1/0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 10 (VLAN0010)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: 11-20
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
```

```
Capture VLANs Allowed: ALL

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

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

show interfaces transceiver

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

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

Syntax Description

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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.
++ : high alarm, +  : high warning, -  : low warning, -- : low alarm.
NA or N/A: not applicable, Tx: transmit, Rx: receive.
mA: milliamperes, dBm: decibels (milliwatts).

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


Device# show interfaces gigabitethernet1/1/1 transceiver properties
  Name : Gi1/1/1
  Administrative Speed: auto
```

```
  Operational Speed: auto
  Administrative Duplex: auto
  Administrative Power Inline: enable
  Operational Duplex: auto
  Administrative Auto-MDIX: off
  Operational Auto-MDIX: off
```

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

```
Device# show interfaces gigabitethernet1/1/1 transceiver detail
  ITU Channel not available (Wavelength not available),
  Transceiver is internally calibrated.
  mA:milliamperes, dBm:decibels (milliwatts), N/A:not applicable.
  ++:high alarm, +:high warning, -:low warning, -- :low alarm.
  A2D readouts (if they differ), are reported in parentheses.
  The threshold values are uncalibrated.

                           High Alarm  High Warn  Low Warn   Low Alarm
           Temperature     Threshold   Threshold  Threshold  Threshold
  Port     (Celsius)      (Celsius)   (Celsius)  (Celsius)  (Celsius)
  -------  -------------  ----------  ---------  ---------  ---------
  Gi1/1/1  29.9           74.0        70.0       0.0        -4.0
                           High Alarm  High Warn  Low Warn   Low Alarm
           Voltage         Threshold   Threshold  Threshold  Threshold
  Port     (Volts)         (Volts)     (Volts)    (Volts)    (Volts)
  -------  ------------    ----------  ---------  ---------  ---------
  Gi1/1/1  3.28            3.60        3.50       3.10       3.00

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

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

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_ER                  ALL
   XENPAK_LR               10-1838-04
```

```
  X2_LR                    ALL
  XFP_LR                   ALL
  XENPAK_LW                ALL
  X2_LW                    ALL
  XFP_LW                   NONE
  XENPAK SR                NONE
  X2 SR                    ALL
  XFP SR                   ALL
  XENPAK LX4               NONE
  X2 LX4                   NONE
  XFP LX4                  NONE
  XENPAK CX4               NONE
  X2 CX4                   NONE
  XFP CX4                  NONE
  SX GBIC                  NONE
  LX GBIC                  NONE
  ZX GBIC                  NONE
  CWDM_SFP                 ALL
  Rx_only_WDM_SFP          NONE
  SX_SFP                   ALL
  LX_SFP                   ALL
  ZX_SFP                   ALL
  EX_SFP                   ALL
  SX SFP                   NONE
  LX SFP                   NONE
  ZX SFP                   NONE
  GIgE BX U SFP            NONE
  GigE BX D SFP            ALL
  X2 LRM                   ALL
  SR_SFPP                  ALL
  LR_SFPP                  ALL
  LRM_SFPP                 ALL
  ER_SFPP                  ALL
  ZR_SFPP                  ALL
  DWDM_SFPP                ALL
  GIgE BX 40U SFP          ALL
  GigE BX 40D SFP          ALL
  GigE BX 40DA SFP         ALL
  GIgE BX 80U SFP          ALL
  GigE BX 80D SFP          ALL
  GIG BXU_SFPP             ALL
  GIG BXD_SFPP             ALL
  GIG BX40U_SFPP           ALL
  GIG BX40D_SFPP           ALL
  GigE Dual Rate LX SFP    ALL
  CWDM_SFPP                ALL
  CPAK_SR10                ALL
  CPAK_LR4                 ALL
  QSFP_LR                  ALL
  QSFP_SR                  ALL
```

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

```
Device# show interfaces transceiver threshold-table
             Optical Tx     Optical Rx    Temp     Laser Bias    Voltage
                                                   current
            -------------  -------------  ------   ------------  ---------

 DWDM GBIC
Min1             -4.00        -32.00        -4           N/A          4.65
Min2              0.00        -28.00        0            N/A          4.75
Max2              4.00         -9.00        70           N/A          5.25
Max1              7.00         -5.00        74           N/A          5.40
 DWDM SFP
```

```
Min1             -4.00        -32.00        -4            N/A           3.00
Min2              0.00        -28.00        0             N/A           3.10
Max2              4.00         -9.00        70            N/A           3.50
Max1              8.00         -5.00        74            N/A           3.60
 RX only WDM GBIC
Min1              N/A         -32.00        -4            N/A           4.65
Min2              N/A         -28.30        0             N/A           4.75
Max2              N/A          -9.00        70            N/A           5.25
Max1              N/A          -5.00        74            N/A           5.40
 DWDM XENPAK
Min1             -5.00        -28.00        -4            N/A           N/A
Min2             -1.00        -24.00        0             N/A           N/A
Max2              3.00         -7.00        70            N/A           N/A
Max1              7.00         -3.00        74            N/A           N/A
 DWDM X2
Min1             -5.00        -28.00        -4            N/A           N/A
Min2             -1.00        -24.00        0             N/A           N/A
Max2              3.00         -7.00        70            N/A           N/A
Max1              7.00         -3.00        74            N/A           N/A
 DWDM XFP
Min1             -5.00        -28.00        -4            N/A           N/A
Min2             -1.00        -24.00        0             N/A           N/A
Max2              3.00         -7.00        70            N/A           N/A
Max1              7.00         -3.00        74            N/A           N/A
 CWDM X2
Min1              N/A           N/A         0             N/A           N/A
Min2              N/A           N/A         0             N/A           N/A
Max2              N/A           N/A         0             N/A           N/A
Max1              N/A           N/A         0             N/A           N/A

<output truncated>
```

Related Commands

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

show macro auto

To display Auto Smartports macro information, use the **show macro auto** command in user EXEC mode.

show macro auto {**address-group** *address-group-name* | **device** [**access-point**] [**ip-camera**] [**lightweight-ap**] [**media-player**] [**phone**] [**router**] [**switch**] | **global** [*event_trigger*] | **interface** [*interface_id*]}

Syntax Description

address-group [*address-group-name*]	Displays address-group information. (Optional) *address-group-name*—Displays information for the specified address group.
device [*access-point*] [*ip-camera*] [*lightweight-ap*] [*media-player*] [*phone*] [*router*] [*switch*]	Displays device information about one or more devices. • (Optional) **access-point**—Autonomous access point • (Optional) **ip-camera**—Cisco IP video surveillance camera • (Optional) **lightweight-ap**—Lightweight access point • (Optional) **media-player**—Digital media player • (Optional) phone—Cisco IP phone • (Optional) **router**—Cisco router • (Optional) **switch**—Cisco switch
global [*event_trigger*]	Displays Auto Smartports information about the switch. (Optional) *event_trigger*—Displays information about the specified event trigger.
interface [*interface_id*]	Displays interface status. (Optional) *interface_id*—isplays information about the specified interface.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Use this command to display the Auto SmartPorts information for the switch. Use the **show macro auto device** command to display the configurable parameters for a device.

Example

This example shows how to use the **show macro auto device** to view the configuration on the switch:

```
Device# show macro auto device
Device:lightweight-ap
Default Macro:CISCO_LWAP_AUTO_SMARTPORT
Current Macro:CISCO_LWAP_AUTO_SMARTPORT
Configurable Parameters:ACCESS_VLAN
Defaults Parameters:ACCESS_VLAN=1
Current Parameters:ACCESS_VLAN=1

Device:access-point
Default Macro:CISCO_AP_AUTO_SMARTPORT
Current Macro:CISCO_AP_AUTO_SMARTPORT
Configurable Parameters:NATIVE_VLAN
Defaults Parameters:NATIVE_VLAN=1
Current Parameters:NATIVE_VLAN=1

Device:phone
Default Macro:CISCO_PHONE_AUTO_SMARTPORT
Current Macro:CISCO_PHONE_AUTO_SMARTPORT
Configurable Parameters:ACCESS_VLAN VOICE_VLAN
Defaults Parameters:ACCESS_VLAN=1 VOICE_VLAN=2
Current Parameters:ACCESS_VLAN=1 VOICE_VLAN=2

Device:router
Default Macro:CISCO_ROUTER_AUTO_SMARTPORT
Current Macro:CISCO_ROUTER_AUTO_SMARTPORT
Configurable Parameters:NATIVE_VLAN
Defaults Parameters:NATIVE_VLAN=1
Current Parameters:NATIVE_VLAN=1

Device:switch
Default Macro:CISCO_SWITCH_AUTO_SMARTPORT
Current Macro:CISCO_SWITCH_AUTO_SMARTPORT
Configurable Parameters:NATIVE_VLAN
Defaults Parameters:NATIVE_VLAN=1
Current Parameters:NATIVE_VLAN=1

Device:ip-camera
Default Macro:CISCO_IP_CAMERA_AUTO_SMARTPORT
Current Macro:CISCO_IP_CAMERA_AUTO_SMARTPORT
Configurable Parameters:ACCESS_VLAN
Defaults Parameters:ACCESS_VLAN=1
Current Parameters:ACCESS_VLAN=1

Device:media-player
Default Macro:CISCO_DMP_AUTO_SMARTPORT
Current Macro:CISCO_DMP_AUTO_SMARTPORT
Configurable Parameters:ACCESS_VLAN
Defaults Parameters:ACCESS_VLAN=1
Current Parameters:ACCESS_VLAN=1
```

This example shows how to use the **show macro auto address-group name** command to view the TEST3 address group configuration on the switch:

```
Device# show macro auto address-group TEST3MAC Address Group Configuration:
```

```
Group Name OUI  MAC ADDRESS
-------------------------------------------------------------
TEST3 2233.33     0022.0022.0022
2233.34
```

show memory platform

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

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

Syntax Description

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

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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
```

```
  VMmalloc Chunk : 1069542588
  VMmalloc Total : 1069547512
  VMmalloc Used  : 2588
  Writeback      : 0
  HugePages Total: 0
  HugePages Free : 0
  HugePages Rsvd : 0
  HugePage Size  : 2048

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

Buffers (kB)     : 437136

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

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

```
Device# show memory platform information

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

 Architecture     : mips64
 Memory (kB)
   Physical       : 3976852
   Total          : 3976852
   Used           : 2761224
   Free           : 1215628
   Active         : 2128060
   Inactive       : 1584444
   Inact-dirty    : 0
   Inact-clean    : 0
   Dirty          : 284
   AnonPages      : 1294656
   Bounce         : 0
   Cached         : 1979644
   Commit Limit   : 1988424
   Committed As   : 3342184
   High Total     : 0
   High Free      : 0
   Low Total      : 3976852
   Low Free       : 1215628
   Mapped         : 516212
   NFS Unstable   : 0
   Page Tables    : 17096
   Slab           : 0
   VMmalloc Chunk : 1069542588
   VMmalloc Total : 1069547512
   VMmalloc Used  : 2588
   Writeback      : 0
   HugePages Total: 0
   HugePages Free : 0
   HugePages Rsvd : 0
   HugePage Size  : 2048
```

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

Buffers (kB)     : 438228

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

show module

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

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

Syntax Description

switch-num	(Optional) Number of the switch.

Command Default

None

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Entering the **show module** command without the *switch-num* argument is the same as entering the show module all command.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

This is an example of output from the **show network-policy profile** command:

```
Device# show network-policy profile
Network Policy Profile 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 parser macro

To display the parameters for all configured macros or for one macro on the switch, use the **show parser macro** command in user EXEC mode.

show parser macro {**brief** | **description** [**interface** *interface-id*] | **name** *macro-name*}

Syntax Description

brief	(Optional) Displays the name of each macro.
description [**interface** *interface-id*]	(Optional) Displays all macro descriptions or the description of a specific interface.
name *macro-name*	(Optional) Displays information about a single macro identified by the macro name.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Example

This is a partial output example from the **show parser macro** command. The output for the Cisco-default macros varies depending on the switch platform and the software image running on the switch:

```
Device# show parser macro
Total number of macros = 6
------------------------------------------------------------------
Macro name : cisco-global
Macro type : default global
# Enable dynamic port error recovery for link state
# failures
errdisable recovery cause link-flap
errdisable recovery interval 60

<output truncated>

------------------------------------------------------------------
Macro name : cisco-desktop
Macro type : default interface
# macro keywords $AVID
# Basic interface - Enable data VLAN only
# Recommended value for access vlan (AVID) should not be 1
switchport access vlan $AVID
switchport mode access

<output truncated>

------------------------------------------------------------------
Macro name : cisco-phone
```

```
Macro type : default interface
# Cisco IP phone + desktop template
# macro keywords $AVID $VVID
# VoIP enabled interface - Enable data VLAN
# and voice VLAN (VVID)
# Recommended value for access vlan (AVID) should not be 1
switchport access vlan $AVID
switchport mode access

<output truncated>

------------------------------------------------------------------
Macro name : cisco-switch
Macro type : default interface
# macro keywords $NVID
# Access Uplink to Distribution
# Do not apply to EtherChannel/Port Group
# Define unique Native VLAN on trunk ports
# Recommended value for native vlan (NVID) should not be 1
switchport trunk native vlan $NVID

<output truncated>

------------------------------------------------------------------
Macro name : cisco-router
Macro type : default interface
# macro keywords $NVID
# Access Uplink to Distribution
# Define unique Native VLAN on trunk ports
# Recommended value for native vlan (NVID) should not be 1
switchport trunk native vlan $NVID

<output truncated>

------------------------------------------------------------------
Macro name : snmp
Macro type : customizable

#enable port security, linkup, and linkdown traps
snmp-server enable traps port-security
snmp-server enable traps linkup
snmp-server enable traps linkdown
#set snmp-server host
snmp-server host ADDRESS
#set SNMP trap notifications precedence
snmp-server ip precedence VALUE

------------------------------------------------------------------
```

This example shows the output from the **show parser macro name** command:

```
Device# show parser macro name standard-switch10
Macro name : standard-switch10
Macro type : customizable
macro description standard-switch10
# Trust QoS settings on VOIP packets
auto qos voip trust
# Allow port channels to be automatically formed
channel-protocol pagp
```

This example shows the output from the **show parser macro brief** command:

```
Device# show parser macro brief
    default global   : cisco-global
    default interface: cisco-desktop
    default interface: cisco-phone
    default interface: cisco-switch
    default interface: cisco-router
    customizable     : snmp
```

This exampe shows the output from the **show parser macro description** command:

```
Device# show parser macro description
Global Macro(s): cisco-global
Interface    Macro Description(s)
---------------------------------------------------------------
Gi1/0/1        standard-switch10
Gi1/0/2       this is test macro
---------------------------------------------------------------
```

This example shows the output from the **show parser macro description interface** command:

```
Device# show parser macro description interface gigabitethernet1/0/2
Interface    Macro Description
---------------------------------------------------------------
Gi1/0/2      this is test macro
---------------------------------------------------------------
```

show platform hardware bluetooth

To display information about Bluetooth interface, use the **show platform hardware bluetooth** command in privileged EXEC mode.

show platform hardware bluetooth

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

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 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**}

Syntax Description

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 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.

cos	The class of service (CoS) number from 0 to 7 to set priority.
pcap *pcap-file-name*	Name of the pcap file in internal flash (flash:). Ensure that the file already exists in flash:.
number *packet-number*	Specifies the packet number in the pcap file.
vlan *vlan-id*	VLAN id of the dot1q header in the simulated packet. The range is 1 to 4096.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.
Cisco IOS XE Fuji 16.9.1	The command was enhanced to support MPLS/ARP/VxLAN packet parameters and trace packets captured in a PCAP file.
Cisco IOS XE Gibraltar 16.10.1	The command was enhanced to support data capture across a stack.

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** *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 150323855361
```

Related Commands

Command	Description
monitor capture interface	Configures monitor capture points specifying an attachment point and the packet flow direction.
monitor capture start	Starts the capture of packet data at a traffic trace point into a buffer.
monitor capture stop	Stops the capture of packet data at a traffic trace point.
monitor capture export	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 **show forward** with **pcap**.

show platform resources

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

show platform resources

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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

Example

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

```
Switch# show platform resources

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

Resource                Usage                Max             Warning         Critical
     State
------------------------------------------------------------------------------------------------

 Control Processor      7.20%                100%            90%             95%
     H
  DRAM                  2701MB(69%)          3883MB          90%             95%
     H
```

show platform software 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

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 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
type=AVC msg=audit(1539222292.586:101): 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(1539222292.586:102): avc:  denied  { read } for  pid=14028 comm="ls"
name="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(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(1539438600.897:120): avc:  denied  { execute_no_trans } for  pid=8300
comm="sh"
path="/tmp/sw/mount/cat9k-rpbase.2018-10-02_00.13_mhungund.SSA.pkg/nyquist/usr/bin/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
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  { 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
type=AVC msg=audit(1539438696.969:125): avc:  denied  { execute_no_trans } for  pid=10057
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(1539438732.973:126): 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(1539438778.008:127): 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(1539438800.156:128): 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
type=AVC msg=audit(1539438834.099:129): 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
type=AVC msg=audit(1539440246.697:149): 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
type=AVC msg=audit(1539440299.119:150): 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 ============
===================================
```

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_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
type=AVC msg=audit(1539222292.586:101): 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(1539222292.586:102): avc:  denied  { read } for  pid=14028 comm="ls"
name="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  { 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
type=AVC msg=audit(1539438696.969:125): avc:  denied  { execute_no_trans } for  pid=10057
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(1539438732.973:126): 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(1539438778.008:127): 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(1539438800.156:128): 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
type=AVC msg=audit(1539438834.099:129): 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
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 ============
===================================
```

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.
punt	Specifies the punt informtion.
cpuq	Specifies information about CPU receive queue.
rates	Specifies the rate at which the packets are punted.

Command Modes

Privileged EXEC (#)

Command History

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

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


Packets per second averaged over 10 seconds, 1 min and 5 mins
================================================================================================
 Q  |          Queue             |  Rx    |  Rx    |  Rx    |  Drop  |  Drop    |  Drop
 no |          Name              |  10s   |  1min  |  5min  |  10s   |  1min    |  5min
================================================================================================
 0  CPU_Q_DOT1X_AUTH                0        0        0        0        0        0
 1  CPU_Q_L2_CONTROL                 0        0        0        0        0        0
 2  CPU_Q_FORUS_TRAFFIC              336      266      320      0        0        0
```

```
 3  CPU_Q_ICMP_GEN                  0         0         0         0         0         0
 4  CPU_Q_ROUTING_CONTROL           0         0         0         0         0         0
 5  CPU_Q_FORUS_ADDR_RESOLUTION     0         0         0         0         0         0
 6  CPU_Q_ICMP_REDIRECT             0         0         0         0         0         0
 7  CPU_Q_INTER_FED_TRAFFIC         0         0         0         0         0         0
 8  CPU_Q_L2LVX_CONTROL_PKT         0         0         0         0         0         0
 9  CPU_Q_EWLC_CONTROL              0         0         0         0         0         0
10 CPU_Q_EWLC_DATA                 0         0         0         0         0         0
11 CPU_Q_L2LVX_DATA_PKT            0         0         0         0         0         0
12 CPU_Q_BROADCAST                 0         0         0         0         0         0
13 CPU_Q_LEARNING_CACHE_OVFL       0         0         0         0         0         0
14 CPU_Q_SW_FORWARDING             0         0         0         0         0         0
15 CPU_Q_TOPOLOGY_CONTROL          0         0         0         0         0         0
16 CPU_Q_PROTO_SNOOPING            0         0         0         0         0         0
17 CPU_Q_DHCP_SNOOPING             0         0         0         0         0         0
18 CPU_Q_TRANSIT_TRAFFIC           0         0         0         0         0         0
19 CPU_Q_RPF_FAILED                0         0         0         0         0         0
20 CPU_Q_MCAST_END_STATION_SERVICE 0         0         0         0         0         0
21 CPU_Q_LOGGING                   0         0         0         0         0         0
22 CPU_Q_PUNT_WEBAUTH              0         0         0         0         0         0
23 CPU_Q_HIGH_RATE_APP             0         0         0         0         0         0
24 CPU_Q_EXCEPTION                 0         0         0         0         0         0
25 CPU_Q_SYSTEM_CRITICAL           0         0         0         0         0         0
26 CPU_Q_NFL_SAMPLED_DATA          0         0         0         0         0         0
27 CPU_Q_LOW_LATENCY               0         0         0         0         0         0
28 CPU_Q_EGR_EXCEPTION             0         0         0         0         0         0
29 CPU_Q_FSS                       0         0         0         0         0         0
30 CPU_Q_MCAST_DATA                0         0         0         0         0         0
31 CPU_Q_GOLD_PKT                  0         0         0         0         0         0
```

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

Table 17: show platform software fed switch active punt cpuq rates Field Descriptions

Field	Description
Queue Name	Name of the queue.
Rx	The rate at which the packets are received per second in 10s, 1 minute and 5 minutes.
Drop	The rate at which the packets are dropped per second in 10s, 1 minute and 5 minutes.

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

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

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

------ Packet Number: 1, Timestamp: 2018/09/04 23:22:10.179 ------
 interface : GigabitEthernet2/0/2 [if-id: 0x00000032] (physical)
 ether hdr : dest mac: 0100.0ccc.cccd, src mac: 2c36.f8fc.4884
 ether hdr : ethertype: 0x0032

 Doppler Frame Descriptor :
```

```
   0000000044004E04  C00F402D94510000  0000000000000100  0000400401000000
   0000000001000050  000000006D000100  0000000025836200  0000000000000000

 Packet Data Dump (length: 68 bytes) :
   01000CCCCCCD2C36  F8FC48840032AAAA  0300000C010B0000  00000080012C36F8
   FC48800000000080  012C36F8FC488080  0400001400020000  0071000000020001
   244E733E

------ Packet Number: 2, Timestamp: 2018/09/04 23:22:10.179 ------
 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 informtion.
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	Modification
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 plataform software fed switch active punt rates interfaces

Punt Rate on Interfaces Statistics

Packets per second averaged over 10 seconds, 1 min and 5 mins

================================================================================================

                              |           |  Rx   |  Rx   |  Rx   | Drop |  Drop  |  Drop
 Interface Name               |  IF_ID    |  10s  |  1min |  5min |  10s |  1min  |  5min
```

```
=================================================================================================

 Vlan3                          0x00000034    1000    1000     520       0       0       0
-------------------------------------------------------------------------------------------------
```

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

Table 18: show platform software fed switch active punt rates interfaces Field Descriptions

Field	Description
Interface Name	Name of the physical interface.
IF_ID	ID of the physical interface.
Rx	The per second rate at which the packets are received in 10s, 1 minute and 5 minutes.
Drop	The per second rate at which the packets are dropped in 10s, 1 minute and 5 minutes.

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)
=================================================================================
 Q  |         Queue                 |  Recv   |  Recv  |  Drop  |  Drop  |
 no |         Name                  |  Total  |  Rate  |  Total |  Rate  |
=================================================================================
 0   CPU_Q_DOT1X_AUTH                      0        0        0        0
 1   CPU_Q_L2_CONTROL                  29519        0        0        0
 2   CPU_Q_FORUS_TRAFFIC                   0        0        0        0
 3   CPU_Q_ICMP_GEN                        0        0        0        0
 4   CPU_Q_ROUTING_CONTROL                 0        0        0        0
 5   CPU_Q_FORUS_ADDR_RESOLUTION           0        0        0        0
 6   CPU_Q_ICMP_REDIRECT                   0        0        0        0
 7   CPU_Q_INTER_FED_TRAFFIC               0        0        0        0
 8   CPU_Q_L2LVX_CONTROL_PKT               0        0        0        0
 9   CPU_Q_EWLC_CONTROL                    0        0        0        0
 10  CPU_Q_EWLC_DATA                       0        0        0        0
 11  CPU_Q_L2LVX_DATA_PKT                  0        0        0        0
 12  CPU_Q_BROADCAST                       0        0        0        0
 13  CPU_Q_LEARNING_CACHE_OVFL             0        0        0        0
 14  CPU_Q_SW_FORWARDING                   0        0        0        0
 15  CPU_Q_TOPOLOGY_CONTROL               98        0        0        0
 16  CPU_Q_PROTO_SNOOPING                  0        0        0        0
 17  CPU_Q_DHCP_SNOOPING                   0        0        0        0
 18  CPU_Q_TRANSIT_TRAFFIC                 0        0        0        0
 19  CPU_Q_RPF_FAILED                      0        0        0        0
```

```
 20  CPU_Q_MCAST_END_STATION_SERVICE        0         0         0         0
 21  CPU_Q_LOGGING                          0         0         0         0
 22  CPU_Q_PUNT_WEBAUTH                     0         0         0         0
 23  CPU_Q_HIGH_RATE_APP                    0         0         0         0
 24  CPU_Q_EXCEPTION                        0         0         0         0
 25  CPU_Q_SYSTEM_CRITICAL                  0         0         0         0
 26  CPU_Q_NFL_SAMPLED_DATA                 0         0         0         0
 27  CPU_Q_LOW_LATENCY                      0         0         0         0
 28  CPU_Q_EGR_EXCEPTION                    0         0         0         0
 29  CPU_Q_FSS                              0         0         0         0
 30  CPU_Q_MCAST_DATA                       0         0         0         0
 31  CPU_Q_GOLD_PKT                         0         0         0         0

------------------------------------------------------------------------------
```

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

Table 19: show platform software fed switch punt rates interfaces interface-id Field Descriptions

Field	Description
Queue Name	Name of the queue.
Recv Total	Total number of packets received.
Recv Rate	Per second rate at which the packets are received.
Drop Total	Total number of packets dropped.
Drop Rate	Per second rate at which the packets are dropped.

show platform software ilpower

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

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

Syntax Description

details	Displays inline power details for all the interfaces.
port	Displays inline power port configuration.
GigabitEthernet *interface-number*	The GigabitEthernet interface number. Values range from 0 to 9.
system *slot-number*	Displays inline power system configuration.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	The command was introduced.

Examples

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

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

```
Power Good:        Stopped
Power Denied:      Stopped
Cisco Powered Device Detect:   Stopped
```

show platform software 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*

Syntax Description

Syntax Description

chunk	(Optional) Displays chunk memory information for the specified process.
database	(Optional) Displays database memory information for the specified process.
messaging	(Optional) Displays messaging memory information for the specified process. The information displayed is for internal debugging purposes only.

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.
- **iomd**—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.

slot

Hardware slot where the process for which the level is set, is running. Options include:

- *number*—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.
- *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.
- **RP standby**—The standby 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 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 Default

No default behavior or values.

Command Modes

Privileged EXEC (#)

Command History

Command History

Release	Modificatio
Cisco IOS XE Fuji 16.9.2	This comm

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
  AOM object              1920374       1920310       4             0
  AOM links array         880379        880315        4             0
  smc_message             819575        819511        4             0
  AOM update state        640380        640316        4             0
  dpidb-config            208776        203544        351           24
  fman-infra-avl          178016        153680        1521          0
  AOM batch               152373        152309        4             0
  AOM asynchronous conte  128388        128324        4             0
  AOM basic data          124824        124760        5             1
  eventutil               118939        118299        50            10
  AOM tree node           96465         96385         5             0
  AOM tree root           72377         72313         4             0
  acl                     36090         31914         504           243
  fman-infra-ipc          35326         24366         115097        114412
  AOM uplink update node  32386         32322         4             0
  unknown                 30528         23808         424           4
  uipeer                  27232         27152         5             0
  fman-infra-qos          26872         24712         164           29
  cce-class               19427         15411         251           0
  l2 control protocol     15472         12896         325           164
  fman-infra-cce          15272         13576         106           0
  smc_channel             15223         15159         4             0
  unknown                 14208         8736          447           105
  chunk                   12513         12033         33            3
  cce-bind                8496          7552          82            23
  MATM mac entry          8040          5928          544           412
  adj                     7064          6312          157           110
  route-pfx               6116          5412          157           113
  Filter_rules            4912          4896          1             0
  fman-infra-dpidb        4130          2338          112           0
  SMC Buffer              3794          3202          43            6
  urpf-list               3028          2100          85            27
  lookup                  2480          2160          30            10
  MATM mac table          2432          1600          148           96
  cdllib                  1688          1672          1             0
  route-tbl               1600          1264          21            0
  FNF Flowdef             1492          1460          3             1
  acl-ref                 1120          1024          8             2
  cgm-lib                 1120          880           410           395
  pbr_if_cfg              1088          976           205           198
  FNF Monitor             1048          1032          1             0
  pbr_routemap            960           864           18            12
!
!
!
```

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

Table 20: show platform software memory brief Field Descriptions

Field	Description
module	Name of submodule.
allocated	Memory, allocated in bytes.
requested	Number of bytes requested by application.
allocs	Number of discrete allocation event attempts.
frees	Number of free events.

show platform software process list

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

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

Syntax Description

switch *switch-number*	Displays information about the switch. Valid values for *switch-number* argument are from 0 to 9.
active	Displays information about the active instance of the switch.
standby	Displays information about the standby instance of the switch.
0	Displays information about the shared port adapters (SPA) Interface Processor slot 0.
F0	Displays information about the Embedded Service Processor (ESP) slot 0.
R0	Displays information about the Route Processor (RP) slot 0.
name *process-name*	(Optional) Displays information about the specified process. 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 EXE (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	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:

```
# show platform software process list switch active R0
Name                    Pid    PPid  Group Id  Status    Priority  Size
------------------------------------------------------------------------------
```

```
systemd                   1       0         1  S              20  4876
kthreadd                  2       0         0  S              20  0
ksoftirqd/0               3       2         0  S              20  0
kworker/0:0H              5       2         0  S               0  0
rcu_sched                 7       2         0  S              20  0
rcu_bh                    8       2         0  S              20  0
migration/0               9       2         0  S      4294967196  0
watchdog/0               10       2         0  S      4294967196  0
watchdog/1               11       2         0  S      4294967196  0
migration/1              12       2         0  S      4294967196  0
ksoftirqd/1              13       2         0  S              20  0
kworker/1:0H             15       2         0  S               0  0
watchdog/2               16       2         0  S      4294967196  0
migration/2              17       2         0  S      4294967196  0
ksoftirqd/2              18       2         0  S              20  0
kworker/2:0H             20       2         0  S               0  0
watchdog/3               21       2         0  S      4294967196  0
migration/3              22       2         0  S      4294967196  0
ksoftirqd/3              23       2         0  S              20  0
kworker/3:0              24       2         0  S              20  0
kworker/3:0H             25       2         0  S               0  0
kdevtmpfs                26       2         0  S              20  0
netns                    27       2         0  S               0  0
perf                     28       2         0  S               0  0
khungtaskd               29       2         0  S              20  0
writeback                30       2         0  S               0  0
ksmd                     31       2         0  S              25  0
khugepaged               32       2         0  S              39  0
crypto                   33       2         0  S               0  0
bioset                   34       2         0  S               0  0
kblockd                  35       2         0  S               0  0
ata_sff                  36       2         0  S               0  0
rpciod                   37       2         0  S               0  0
kswapd0                  63       2         0  S              20  0
vmstat                   64       2         0  S               0  0
fsnotify_mark            65       2         0  S              20  0
nfsiod                   66       2         0  S               0  0
.
.
.
```

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

Table 21: show platform software process list Field Descriptions

Field	Description
Name	Displays the command name associated with the process. Different threads in the same process may have different command values.
Pid	Displays the process ID that is used by the operating system to identify and keep track of the processes.
PPid	Displays process ID of the parent process.
Group Id	Displays the group ID
Status	Displays the process status in human readable form.

Field	Description
Priority	Displays the negated scheduling priority.
Size	Prior to Cisco IOS XE Gibraltar 16.10.1: Displays Virtual Memory size. 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.

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.

show platform 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

switch *switch-number*	Displays information about the switch. Enter the switch number.
active	Specifies the active instance of the device.
standby	Specifies the standby instance of the device.
0	Specifies the Shared Port Adapter (SPA) Interface Processor slot 0.
F0	Specifies the Embedded Service Processor (ESP) slot 0.
FP	Specifies the Embedded Service Processor (ESP).
R0	Specifies the Route Processor (RP) slot 0.
all	Lists all processes.
sorted	(Optional) Sorts the output based on Resident Set Size (RSS).
virtual	(Optional) Specifies virtual memory.
name *process-name*	Specifies a process name.
maps	Specifies the memory maps of a process.
smaps summary	Specifies the smaps summary of a process.
process-id *process-id*	Specifies a process identifier.

Command History

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

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

   Pid        RSS        PSS       Heap     Shared    Private              Name
-------------------------------------------------------------------------------
     1       4876       3229       1064       1808       3068           systemd
   118       3184       1327        132       2352        832   systemd-journal
   159       3008       1191        396       1996       1012     systemd-udevd
   407       3192       1262        132       2196        996       dbus-daemon
  3406       4772       3064        264       1940       2832          virtlogd
  3411       5712       3474       2964       2344       3368       droputil.sh
  3416       2588        358        132       2336        252       libvirtd.sh
  3420       5708       3484       2976       2308       3400      reflector.sh
  3424       1804        263        132       1632        172            xinetd
  3425        964        118        132        872         92             sleep
  3434       3060        844        528       2304        756            oom.sh
  3442       2068        606        132       1604        464           rpcbind
  3485       2380        845        132       1636        744         rpc.statd
  3486       1632        338        132       1348        284   boothelper_evt.
  3493       1136        156        132       1004        132      inotifywait
  3504       2048        753        132       1372        676       rpc.mountd
  3584       2868        620         36       2384        484            rotee
  3649       1032        116        132        944         88             sleep
  3705       2784        613         36       2296        488            rotee
  3718       2856        610         36       2376        480            rotee
  3759       1292        184        132       1136        156      inotifywait
  3787       4256       2040       1640       2300       1956          iptbl.sh
  3894       2948        637         36       2460        488            rotee
  4017       1380        175        132       1236        144      inotifywait
  4866       1820        287        132       1624        196           xinetd
  5887       1692        257        132       1508        184           xinetd
  5891       7248       4984       4584       2348       4900   rollback_timer.
  5893       1764        257        132       1588        176           xinetd
  6031       2804        601         36       2332        472            rotee
  6037       1228        163        132       1092        136      inotifywait
  6077       4736       3389       2992       1368       3368          psvp.sh
  6115       1620        476         36       1152        468            rotee
  6122        624        149        132        480        144      inotifywait
  6127       5440       4077       3680       1384       4056           pvp.sh
  6165       1736        592         36       1152        584            rotee
  6245        624        149        132        480        144      inotifywait
  6353       2592       1260        924       1352       1240          pman.sh
  6470       1632        488         36       1152        480            rotee
  6499       2588       1262        924       1348       1240          pman.sh
  6666       1640        496         36       1152        488            rotee
  6718       2584       1258        800       1348       1236          pman.sh
  6736       8360       7020       6640       1360       7000   auto_upgrade_cl
  6909       1636        492         36       1152        484            rotee
  6955       2588       1262        928       1348       1240          pman.sh
  7029       2196        679         40       1552        644   auto_upgrade_se
  7149       1636        492         36       1152        484            rotee
  7224      13200       4595         48       9368       3832        bt_logger
  7295       2588       1262        800       1348       1240          pman.sh
.
.
.
```

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

Table 22: show platform software process memory Field Descriptions

Field	Description
PID	Displays the process ID that is used by the operating system to identify and keep track of the processes.
RSS	Displays the Resident Set Size (in kilobytes (KB)) that shows how much memory is allocated to that process in the RAM.
PSS	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.
Heap	Displays where all user-allocated memory is located.
Shared	Shared clean + Shared dirty
Private	Private clean + Private dirty
Name	Displays the command name associated with the process. Different threads in the same process may have different command values.

show platform software process slot switch

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

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

Syntax Description

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

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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

Examples

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

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

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

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

Related Commands

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

show platform software status control-processor

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

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

Syntax Description

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

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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)
```

```
  User:  4.50, System:  1.20, Nice:  0.00, Idle: 94.20
  IRQ:  0.00, SIRQ:  0.10, IOwait:  0.00
CPU1: CPU Utilization (percentage of time spent)
  User:  5.20, System:  0.50, Nice:  0.00, Idle: 94.29
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU2: CPU Utilization (percentage of time spent)
  User:  3.60, System:  0.70, Nice:  0.00, Idle: 95.69
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU3: CPU Utilization (percentage of time spent)
  User:  3.00, System:  0.60, Nice:  0.00, Idle: 96.39
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00

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

9-RP0: unknown, statistics updated 4 seconds ago
Load Average: healthy
  1-Min: 0.20, status: healthy, under 5.00
  5-Min: 0.35, status: healthy, under 5.00
  15-Min: 0.35, status: healthy, under 5.00
Memory (kb): healthy
  Total: 3976852
  Used: 1451328 (36%), status: healthy
  Free: 2525524 (64%)
  Committed: 1675932 (42%), under 95%
Per-core Statistics
CPU0: CPU Utilization (percentage of time spent)
  User:  1.90, System:  0.50, Nice:  0.00, Idle: 97.60
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU1: CPU Utilization (percentage of time spent)
  User:  4.39, System:  0.19, Nice:  0.00, Idle: 95.40
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU2: CPU Utilization (percentage of time spent)
  User:  5.70, System:  1.00, Nice:  0.00, Idle: 93.30
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU3: CPU Utilization (percentage of time spent)
  User:  1.30, System:  0.60, Nice:  0.00, Idle: 98.00
  IRQ:  0.00, SIRQ:  0.10, IOwait:  0.00
```

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

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

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

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

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

show 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

switch *switch-number*	Displays information about the switch. Enter the switch number.
active	Specifies the active instance of the device.
standby	Specifies standby instance of the device.
0	Specifies the Shared Port Adapter (SPA) Interface Processor slot 0.
F0	Specifies the Embedded Service Processor (ESP) slot 0.
FP active	Specifies the active instance of Embedded Service Processor (ESP).
R0	Specifies the Route Processor (RP) slot 0.
pname	Specifies a process name. The possible values are **cdman**, **vidman**, and **all**.
tname	Specifies a thread name. The possible values are **main**, **pktio**, **rt**, and **all**.

Command History

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

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    Vcswch   Nvcswch  Status    Priority
TIME+  Size
-------------------------------------------------------------------------------------------------
cdman         8407    7295      8407     1         0         0  S               20
12309  36976
```

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

Table 23: show platform software thread list Field Descriptions

Field	Description
Name	Displays the command name associated with the process. Different threads in the same process may have different command values.
Tid	Displays the process ID.
PPid	Displays the process ID of the parent process.
Group Id	Displays the group ID.
Core	Displays processor information.
Vcswch	Displays the number of voluntary context switches.
Nvcswch	Displays the number of non-voluntary context switches.
Status	Displays the process status in human readable form.
Priority	Displays the negated scheduling priority.
TIME+	Displays the time since the start of the process.
Size	Displays the Resident Set Size (in kilobytes (KB)) that shows how much memory is allocated to that process in the RAM.

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

sorted	(Optional) Displays output sorted based on percentage of CPU usage on a platform.
1min	(Optional) Sorts based on 1 minute intervals.
5min	(Optional) Sorts based on 5 minute intervals.
5sec	(Optional) Sorts based on 5 second intervals.
location	Specifies the Field Replaceable Unit (FRU) location.
switch *switch-number*	Displays information about the switch. Enter the switch number.
active	Specifies the active instance of the device.
standby	Specifies the standby instance of the device.
F0	Specifies the Embedded Service Processor (ESP) slot 0.
FP active	Specifies active instances on the Embedded Service Processor (ESP).
R0	Specifies the Route Processor (RP) slot 0.
RP active	Specifies active instances on the Route Processor (RP).

Command History

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

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
```

```
     2       0      0%      0%      0%  S                0  kthreadd
     3       2      0%      0%      0%  S                0  ksoftirqd/0
     5       2      0%      0%      0%  S                0  kworker/0:0H
     7       2      0%      0%      0%  S                0  rcu_sched
     8       2      0%      0%      0%  S                0  rcu_bh
     9       2      0%      0%      0%  S                0  migration/0
    10       2      0%      0%      0%  S                0  watchdog/0
    11       2      0%      0%      0%  S                0  watchdog/1
    12       2      0%      0%      0%  S                0  migration/1
    13       2      0%      0%      0%  S                0  ksoftirqd/1
    15       2      0%      0%      0%  S                0  kworker/1:0H
    16       2      0%      0%      0%  S                0  watchdog/2
    17       2      0%      0%      0%  S                0  migration/2
    18       2      0%      0%      0%  S                0  ksoftirqd/2
    20       2      0%      0%      0%  S                0  kworker/2:0H
    21       2      0%      0%      0%  S                0  watchdog/3
    22       2      0%      0%      0%  S                0  migration/3
    23       2      0%      0%      0%  S                0  ksoftirqd/3
    24       2      0%      0%      0%  S                0  kworker/3:0
    25       2      0%      0%      0%  S                0  kworker/3:0H
    26       2      0%      0%      0%  S                0  kdevtmpfs
    27       2      0%      0%      0%  S                0  netns
    28       2      0%      0%      0%  S                0  perf
    29       2      0%      0%      0%  S                0  khungtaskd
    30       2      0%      0%      0%  S                0  writeback
    31       2      7%      8%      8%  S                0  ksmd
    32       2      0%      0%      0%  S                0  khugepaged
    33       2      0%      0%      0%  S                0  crypto
    34       2      0%      0%      0%  S                0  bioset
    35       2      0%      0%      0%  S                0  kblockd
    36       2      0%      0%      0%  S                0  ata_sff
    37       2      0%      0%      0%  S                0  rpciod
    63       2      0%      0%      0%  S                0  kswapd0
    64       2      0%      0%      0%  S                0  vmstat
    65       2      0%      0%      0%  S                0  fsnotify_mark
.
.
.
```

The following is sample output from the **show processes cpu platform sorted 5min location switch 5 R0**

```
Device# show processes cpu platform sorted 5min location switch 5 R0

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%
   Pid    PPid    5Sec    1Min    5Min  Status        Size  Name
------------------------------------------------------------------------------
 16358   15516      4%      4%      4%  S           221376  fed main event
 14062   12756      1%      1%      1%  S            52140  sif_mgr
 32105    8618      0%      0%      0%  S              260  inotifywait
 31396   31393      0%      0%      0%  S            36516  python2.7
 31393   31271      0%      0%      0%  S             2744  rdope.sh
 31319       1      0%      0%      0%  S             2648  rotee
 31271       1      0%      0%      0%  S             3852  pman.sh
 29671       2      0%      0%      0%  S                0  kworker/u16:0
 29341   29329      0%      0%      0%  S             1780  sntp
 29329       1      0%      0%      0%  S             2788  stack_sntp.sh
.
```

.
.

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%
   Pid    PPid    5Sec    1Min    5Min  Status        Size  Name
--------------------------------------------------------------------------------
     1       0      0%      0%      0%  S             8044  systemd
     2       0      0%      0%      0%  S                0  kthreadd
.
.
.
```

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** }

1min	(Optional) Displays CPU utilization history with 1 minute intervals.
5min	(Optional) Displays CPU utilization history with 5 minute intervals.
5sec	(Optional) Displays CPU utilization history with 5 second intervals.
60min	(Optional) Displays CPU utilization history with 60 minute intervals.
location	Specifies the Field Replaceable Unit (FRU) location.
switch *switch-number*	Displays information about the switch. Enter the switch number.
active	Specifies the active instance of the device.
standby	Specifies the standby instance of the device.
0	Specifies the Shared Port Adapter (SPA) Interface Processor slot 0.
F0	Specifies the Embedded Service Processor (ESP) slot 0.
FP active	Specifies active instances on the Embedded Service Processor (ESP).
R0	Specifies the Route Processor (RP) slot 0.

Command History

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

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
     2       0      0%      0%      0%  S                0  kthreadd
     3       2      0%      0%      0%  S                0  ksoftirqd/0
     5       2      0%      0%      0%  S                0  kworker/0:0H
     7       2      0%      0%      0%  S                0  rcu_sched
     8       2      0%      0%      0%  S                0  rcu_bh
     9       2      0%      0%      0%  S                0  migration/0
    10       2      0%      0%      0%  S                0  watchdog/0
    11       2      0%      0%      0%  S                0  watchdog/1
    12       2      0%      0%      0%  S                0  migration/1
    13       2      0%      0%      0%  S                0  ksoftirqd/1
    15       2      0%      0%      0%  S                0  kworker/1:0H
    16       2      0%      0%      0%  S                0  watchdog/2
    17       2      0%      0%      0%  S                0  migration/2
    18       2      0%      0%      0%  S                0  ksoftirqd/2
    20       2      0%      0%      0%  S                0  kworker/2:0H
    21       2      0%      0%      0%  S                0  watchdog/3
    22       2      0%      0%      0%  S                0  migration/3
    23       2      0%      0%      0%  S                0  ksoftirqd/3
    24       2      0%      0%      0%  S                0  kworker/3:0
    25       2      0%      0%      0%  S                0  kworker/3:0H
    26       2      0%      0%      0%  S                0  kdevtmpfs
    27       2      0%      0%      0%  S                0  netns
    28       2      0%      0%      0%  S                0  perf
    29       2      0%      0%      0%  S                0  khungtaskd
    30       2      0%      0%      0%  S                0  writeback
    31       2      7%      8%      8%  S                0  ksmd
    32       2      0%      0%      0%  S                0  khugepaged
    33       2      0%      0%      0%  S                0  crypto
    34       2      0%      0%      0%  S                0  bioset
    35       2      0%      0%      0%  S                0  kblockd
    36       2      0%      0%      0%  S                0  ata_sff
    37       2      0%      0%      0%  S                0  rpciod
    63       2      0%      0%      0%  S                0  kswapd0
    64       2      0%      0%      0%  S                0  vmstat
    65       2      0%      0%      0%  S                0  fsnotify_mark
.
.
.
```

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: 1%
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 displays information about the CPU utilization of the IOS-XE processes, use the **show processes cpu platform monitor** command in privileged EXEC mode.

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

Syntax Description

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

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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

Examples

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

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

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

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
 6294 root      20   0  3448 1368  912 R    9  0.0   0:00.07 top
17546 root      20   0 2044m 244m  79m S    7  6.3 187:02.07 fed main event
30276 root      20   0  171m  42m  33m S    7  1.1 125:15.54 repm
   16 root      20   0     0    0    0 S    5  0.0  22:07.92 rcuc/2
   21 root      20   0     0    0    0 R    5  0.0  22:13.24 rcuc/3
```

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

Related Commands

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

show processes memory

To display the amount of memory used by each system process, use the **show processes memory** command in privileged EXEC mode.

show processes memory [{ *process-id* | **sorted** [{ **allocated** | **getbufs** | **holding** }] }]

Syntax Description

process-id	(Optional) Process ID (PID) of a specific process. When you specify a process ID, only details for the specified process will be shown.
sorted	(Optional) Displays memory data sorted by the Allocated, Get Buffers, or Holding column. If the **sorted** keyword is used by itself, data is sorted by the Holding column by default.
allocated	(Optional) Displays memory data sorted by the Allocated column.
getbufs	(Optional) Displays memory data sorted by the Getbufs (Get Buffers) column.
holding	(Optional) Displays memory data sorted by the Holding column. This keyword is the default.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The **show processes memory** command and the **show processes memory sorted** command displays a summary of total, used, and free memory, followed by a list of processes and their memory impact.

If the standard **show processes memory** *process-id* command is used, processes are sorted by their PID. If the **show processes memory sorted** command is used, the default sorting is by the Holding value.

Note Holding memory of a particular process can be allocated by other processes also, and so it can be greater than the allocated memory.

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

```
Device# show processes memory

Processor Pool Total:   25954228 Used:    8368640 Free:   17585588
 PID TTY  Allocated      Freed    Holding    Getbufs    Retbufs Process
   0   0    8629528     689900    6751716          0          0 *Init*
   0   0      24048      12928      24048          0          0 *Sched*
   0   0        260        328         68     350080          0 *Dead*
   1   0          0          0      12928          0          0 Chunk Manager
   2   0        192        192       6928          0          0 Load Meter
   3   0     214664        304     227288          0          0 Exec
   4   0          0          0      12928          0          0 Check heaps
   5   0          0          0      12928          0          0 Pool Manager
   6   0        192        192      12928          0          0 Timers
   7   0        192        192      12928          0          0 Serial Backgroun
```

```
  8   0        192        192      12928          0          0 AAA high-capacit
  9   0          0          0      24928          0          0 Policy Manager
 10   0          0          0      12928          0          0 ARP Input
 11   0        192        192      12928          0          0 DDR Timers
 12   0          0          0      12928          0          0 Entity MIB API
 13   0          0          0      12928          0          0 MPLS HC Counter
 14   0          0          0      12928          0          0 SERIAL A'detect
.
.
.
 78   0          0          0      12992          0          0 DHCPD Timer
 79   0        160          0      13088          0          0 DHCPD Database
                                 8329440 Total
```

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

Table 24: show processes memory Field Descriptions

Field	Description
Processor Pool Total	Total amount of memory, in kilobytes (KB), held for the Processor memory pool.
Used	Total amount of used memory, in KB, in the Processor memory pool.
Free	Total amount of free memory, in KB, in the Processor memory pool.
PID	Process ID.
TTY	Terminal that controls the process.
Allocated	Bytes of memory allocated by the process.
Freed	Bytes of memory freed by the process, regardless of who originally allocated it.
Holding	Amount of memory, in KB, currently allocated to the process. This includes memory allocated by the process and assigned to the process.
Getbufs	Number of times the process has requested a packet buffer.
Retbufs	Number of times the process has relinquished a packet buffer.
Process	Process name.
Init	System initialization process.
Sched	The scheduler process.
Dead	Processes as a group that are now dead.
<value> Total	Total amount of memory, in KB, held by all processes (sum of the “Holding” column).

The following is sample output from the **show processes memory** command when the **sorted** keyword is used. In this case, the output is sorted by the Holding column, from largest to smallest.

```
Device# show processes memory sorted

Processor Pool Total:   25954228 Used:    8371280 Free:   17582948
 PID TTY  Allocated      Freed    Holding    Getbufs    Retbufs Process
   0   0    8629528     689900    6751716          0          0 *Init*
```

```
  3   0     217304        304     229928          0          0 Exec
 53   0     109248        192      96064          0          0 DHCPD Receive
 56   0          0          0      32928          0          0 COPS
 19   0      39048          0      25192          0          0 Net Background
 42   0          0          0      24960          0          0 L2X Data Daemon
 58   0        192        192      24928          0          0 X.25 Background
 43   0        192        192      24928          0          0 PPP IP Route
 49   0          0          0      24928          0          0 TCP Protocols
 48   0          0          0      24928          0          0 TCP Timer
 17   0        192        192      24928          0          0 XML Proxy Client
  9   0          0          0      24928          0          0 Policy Manager
 40   0          0          0      24928          0          0 L2X SSS manager
 29   0          0          0      24928          0          0 IP Input
 44   0        192        192      24928          0          0 PPP IPCP
 32   0        192        192      24928          0          0 PPP Hooks
 34   0          0          0      24928          0          0 SSS Manager
 41   0        192        192      24928          0          0 L2TP mgmt daemon
 16   0        192        192      24928          0          0 Dialer event
 35   0          0          0      24928          0          0 SSS Test Client
--More--
```

The following is sample output from the **show processes memory** command when a process ID (*process-id*) is specified:

```
Device# show processes memory 1

Process ID: 1
Process Name: Chunk Manager
Total Memory Held: 8428 bytes
Processor memory holding = 8428 bytes
pc = 0x60790654, size =      6044, count =    1
pc = 0x607A5084, size =      1544, count =    1
pc = 0x6076DBC4, size =       652, count =    1
pc = 0x6076FF18, size =       188, count =    1
I/O memory holding = 0 bytes

Device# show processes memory 2

Process ID: 2
Process Name: Load Meter
Total Memory Held: 3884 bytes
Processor memory holding = 3884 bytes
pc = 0x60790654, size =      3044, count =    1
pc = 0x6076DBC4, size =       652, count =    1
pc = 0x6076FF18, size =       188, count =    1
I/O memory holding = 0 bytes
```

Related Commands

Command	Description
show memory	Displays statistics about memory, including memory-free pool statistics.
show processes	Displays information about the active processes.

show processes memory platform

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

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

Syntax Description

accounting	(Optional) Displays the top memory allocators for each Cisco IOS XE process.
detailed	(Optional) Displays detailed memory information for a specified Cisco IOS XE process.
name *process-name*	(Optional) Displays the Cisco IOS XE process name. Enter the process name.
process-id *process-ID*	(Optional) Displayss the Cisco IOS XE process ID. Enter the process ID.
location	(Optional) Displays information about the Field Replaceable Unit (FRU) location.
maps	(Optional) Displays memory maps of a process.
smaps	(Optional) Displays static memory maps of a process.
sorted	(Optional) Displays the sorted output based on the Resident Set Size (RSS) memory used by Cisco IOS XE process.
switch *switch-number*	Displays information about the device.
active	Displays information about the active instance of the device.
standby	Displays information about the standby instance of the device.
0	Displays information about Shared Port Adapter (SPA)-Inter-Processor slot 0.
F0	Displays information about Embedded Service Processor (ESP) slot 0.
R0	Displays information about Route Processor (RP) slot 0.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.
Cisco IOS XE Gibraltar 16.10.1	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
   Pid    Text      Data   Stack   Dynamic       RSS                  Name
--------------------------------------------------------------------------------
     1    1246      4400     132      1308      4400               systemd
    96     233      2796     132       132      2796       systemd-journal
   105     284      1796     132       176      1796         systemd-udevd
   707      52      2660     132       172      2660            in.telnetd
   744     968      3264     132      1700      3264             brelay.sh
   835      52      2660     132       172      2660            in.telnetd
   863     968      3264     132      1700      3264             brelay.sh
   928     968      3996     132      2312      3996          reflector.sh
   933     968      3976     132      2312      3976           droputil.sh
   934     968      2140     132       528      2140                oom.sh
   936     173       936     132       132       936               xinetd
   945     968      1472     132       132      1472           libvirtd.sh
   947     592     43164     132      3096     43164                 repm
   954      45       932     132       132       932              rpcbind
   986     482      3476     132       132      3476             libvirtd
   988      66       940     132       132       940             rpc.statd
   993     968       928     132       132       928       boothelper_evt.
  1017      21       640     132       132       640           inotifywait
  1089     102      1200     132       132      1200            rpc.mountd
  1328       9      2940     132       148      2940                rotee
  1353      39       532     132       132       532                sleep
!
!
!
```

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

```
device# show processes memory platform accounting
Hourly Stats

  process                 callsite_ID(bytes)  max_diff_bytes   callsite_ID(calls)
max_diff_calls   tracekey                                    timestamp(UTC)

------------------------------------------------------------------------------------------------------------------

  smand_rp_0              3624155137          172389           3624155138          50
         1#a3e0e4361082c702e5bf1afbd90e6313       2018-09-04 14:23
  linux_iosd-imag_rp_0    3626295305          49188            3624155138          12
         1#545420bd869d25eb5ab826182ee5d9ce       2018-09-04 12:03
  btman_rp_0              3624737792          17080            2953915394          64
         1#d6888bd9564a3c4fcf049c31ba07a036       2018-09-04 22:29
```

```
  fman_fp_image_fp_0      3624059905          16960            4027402242          298
         1#921ba4d9df5b0a6e946a3b270bd6592d       2018-09-04 22:55
  fed_main_event_fp_0     3626295305          16396            4027402242          32
         1#27083f7bf3985d892505806cae2bfb0d       2018-09-04 12:03
  dbm_rp_0                3626295305          16396            4027402242          3
         1#2b878f802bd7703c5298d37e7a4e8ac3       2018-09-04 12:02
  tamd_proc_rp_0          3895208962          12632            3624667171          7
         1#5b0ed8f88ef5f873abcaf8a744037a44       2018-09-04 18:47
  btman_fp_0              3624233985          12288            3624737792          9
         1#d6888bd9564a3c4fcf049c31ba07a036       2018-09-04 15:23
  sif_mgr_rp_0            3624059907          8216             4027402242          4
         1#de2a951a8a7bae83ca2c04c56810eb72       2018-09-04 14:21
  python2.7_fp_0          2954560513          8000             2954560513          1
                                                   2018-09-04 12:16
  nginx_rp_0              3357041665          4608             4027402242          4
         1#32e56bb09e0509c5fa5ac32093631206       2018-09-04 16:18
  rotee_FRU_SLOT_NUM      3624667169          4097             3624667169          1
         1#ff68e5150a698cd59fa259828614995b       2018-09-04 10:43
  hman_rp_0               3893617664          1488             3893617664          1
         1#1c4aadada30083c5d6f66dc8ca8cd4cb       2018-09-04 10:42
  tams_proc_rp_0          3895096320          1024             3895096320          1
         1#a36a3afa9884c8dc4d40af1e80cacd26       2018-09-04 10:42
  stack_mgr_rp_0          4027402242          904              4027402242          4
         1#ca902eab11a18ab056b16554f49871e8       2018-09-04 14:21
  sessmgrd_rp_0           3491618816          848              3624155138          8
         1#720239fc8bddcabc059768c55a1640ed       2018-09-04 14:32
  psd_rp_0                4027402242          696              4027402242          4
         1#98cf04e0ddd78c2400b3ca3b5f298594       2018-09-04 14:21
  lman_rp_0               4027402242          592              4027402242          4
         1#dc8ed9e428d36477a617d56c51d5caf2       2018-09-04 14:21
  bt_logger_rp_0          4027402242          592              4027402242          4
         1#ba882be1ed783e72575e97cc0908e0e8       2018-09-04 14:21
  repm_rp_0               4027402242          592              4027402242          4
         1#ae461a05430efa767427f2ab40aba372       2018-09-04 14:21
  fman_rp_rp_0            4027402242          592              4027402242          3
         1#09def9cc1390911be9e3a7a9c89f4cf7       2018-09-04 12:16
  epc_ws_liaison_fp_0     4027402242          592              4027402242          4
         1#41451626dcce9d1478b22e2ebbbdcf54       2018-09-04 14:21
  cli_agent_rp_0          4027402242          592              4027402242          4
         1#92d3882919daf3a9e210807c61de0552       2018-09-04 14:21
  cmm_rp_0                4027402242          592              4027402242          4
         1#15ed1d79e96874b1e0621c42c3de6166       2018-09-04 14:21
  tms_rp_0                4027402242          352              4027402242          4
         1#5c6efe2e21f15aa16318576d3ec9153c       2018-09-04 12:03
  plogd_rp_0              4027402242          48               4027402242          1
         1#2d7f2ef57206f4fa763d7f2f5400bf1b       2018-09-04 10:43
  cmand_rp_0              3624155137          17               3624155137          1
         1#f1f41f61c44d73014023db5d8a46ecf5       2018-09-04 10:42
!
!
!
```

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

```
device# show processes memory platform sorted
System memory: 3976852K total, 2762884K used, 1213968K free,
Lowest: 1213968K

   Pid      Text      Data   Stack   Dynamic       RSS                Name
--------------------------------------------------------------------------
  7885    149848     684864    136        80    684864     linux_iosd-imag
  9655      3787     264964    136     18004    264964                wcm
```

```
  17261      324       248588    132     103908    248588       fed main event
  4268       391       102084    136       5596    102084            cli_agent
  4856       357        93388    132       3680     93388                 dbm
17067     1087       77912    136      1796     77912        platform_mgr
!
!
!
```

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

   Pid      Text      Data   Stack   Dynamic       RSS                Name
--------------------------------------------------------------------------------
  7885    149848     684864    136        80    684864     linux_iosd-imag
  9655      3787     264964    136     18004    264964                 wcm
  17261     324       248588    132     103908    248588       fed main event
  4268       391       102084    136       5596    102084            cli_agent
  4856       357        93388    132       3680     93388                 dbm
17067     1087       77912    136      1796     77912        platform_mgr
!
!
!
```

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**}]

detailed	(Optional) Displays detailed information of the specified IOS-XE process.
name *process-name*	(Optional) Specifies the process name.
location	(Optional) Specifies the Field Replaceable Unit (FRU) location.
switch *switch-number*	(Optional) Displays information about the switch.
active	(Optional) Specifies the active instance of the device.
standby	(Optional) Specifies standby instance of the device.
0	Specifies the Shared Port Adapter (SPA) Interface Processor slot 0.
F0	Specifies the Embedded Service Processor (ESP) slot 0.
FP active	Specifies the active instance in the Embedded Service Processor (ESP).
R0	Specifies the Route Processor (RP) slot 0.

Command History

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

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%
   Pid    PPid  Status        Size  Name
-----------------------------------------------------------
     1       0  S             4876  systemd
     2       0  S                0  kthreadd
     3       2  S                0  ksoftirqd/0
     5       2  S                0  kworker/0:0H
     7       2  S                0  rcu_sched
     8       2  S                0  rcu_bh
     9       2  S                0  migration/0
    10       2  S                0  watchdog/0
    11       2  S                0  watchdog/1
    12       2  S                0  migration/1
```

```
 13       2  S                0  ksoftirqd/1
 15       2  S                0  kworker/1:0H
 16       2  S                0  watchdog/2
 17       2  S                0  migration/2
 18       2  S                0  ksoftirqd/2
 20       2  S                0  kworker/2:0H
 21       2  S                0  watchdog/3
 22       2  S                0  migration/3
 23       2  S                0  ksoftirqd/3
 24       2  S                0  kworker/3:0
 25       2  S                0  kworker/3:0H
 26       2  S                0  kdevtmpfs
 27       2  S                0  netns
 28       2  S                0  perf
 29       2  S                0  khungtaskd
 30       2  S                0  writeback
 31       2  S                0  ksmd
 32       2  S                0  khugepaged
 33       2  S                0  crypto
 34       2  S                0  bioset
 35       2  S                0  kblockd
 36       2  S                0  ata_sff
 37       2  S                0  rpciod
 63       2  S                0  kswapd0
 64       2  S                0  vmstat
 65       2  S                0  fsnotify_mark
 66       2  S                0  nfsiod
 74       2  S                0  bioset
 75       2  S                0  bioset
 76       2  S                0  bioset
 77       2  S                0  bioset
 78       2  S                0  bioset
 79       2  S                0  bioset
 80       2  S                0  bioset
 81       2  S                0  bioset
 82       2  S                0  bioset
 83       2  S                0  bioset
 84       2  S                0  bioset
 85       2  S                0  bioset
 86       2  S                0  bioset
 87       2  S                0  bioset
 88       2  S                0  bioset
 89       2  S                0  bioset
 90       2  S                0  bioset
 91       2  S                0  bioset
 92       2  S                0  bioset
 93       2  S                0  bioset
 94       2  S                0  bioset
 95       2  S                0  bioset
 96       2  S                0  bioset
 97       2  S                0  bioset
100       2  S                0  ipv6_addrconf
102       2  S                0  deferwq
```

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

Table 25: show processes platform Field Descriptions

Field	Description
Pid	Displays the process ID.

Field	Description
PPid	Displays the process ID of the parent process.
Status	Displays the process status in human readable form.
Size	Displays the Resident Set Size (in kilobytes (KB)) that shows how much memory is allocated to that process in the RAM.
Name	Displays the command name associated with the process. Different threads in the same process may have different command values.

show shell

To display shell information, use the **show shell** command in user EXEC mode.

show shell [{**enviornment** | **functions** [{**brief** *shell_function*}] | **triggers**}]

Syntax Description

environment	(Optional) Displays shell environment info
functions [**brief** |*shell_function*]	(Optional) Displays macro information. • **brief**—Names of the shell functions. • *shell_function*—Name of a shell func
triggers	(Optional) Displays event trigger informat

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Use this command to display the shell information for the switch.

Example

This example shows how to use the **show shell** *triggers* command to view the event triggers in the switch software:

```
Device# term shell
Device# show shell triggers
User defined triggers
---------------------
Built-in triggers
-----------------
Trigger Id: CISCO_CUSTOM_EVENT
Trigger description: Custom macroevent to apply user defined configuration
Trigger environment: User can define the macro
Trigger mapping function: CISCO_CUSTOM_AUTOSMARTPORT

Trigger Id: CISCO_DMP_EVENT
Trigger description: Digital media-player device event to apply port configuration
Trigger environment: Parameters that can be set in the shell - $ACCESS_VLAN=(1)
 The value in the parenthesis is a default value
Trigger mapping function: CISCO_DMP_AUTO_SMARTPORT

Trigger Id: CISCO_IPVSC_EVENT
Trigger description: IP-camera device event to apply port configuration
Trigger environment: Parameters that can be set in the shell - $ACCESS_VLAN=(1)
 The value in parenthesis is a default value
Trigger mapping function: CISCO_IP_CAMERA_AUTO_SMARTPORT
```

```
Trigger Id: CISCO_LAST_RESORT_EVENT
Trigger description: Last resortevent to apply port configuration
Trigger environment: Parameters that can be set in the shell - $ACCESS_VLAN=(1)
 The value in the parenthesis is a default value
Trigger mapping function: CISCO_LAST_RESORT_SMARTPORT

Trigger Id: CISCO_PHONE_EVENT
Trigger description: IP-phone device event to apply port configuration
Trigger environment: Parameters that can be set in the shell - $ACCESS_VLAN=(1)
and $VOICE_VLAN=(2), The value in the parenthesis is a default value
Trigger mapping function: CISCO_PHONE_AUTO_SMARTPORT

Trigger Id: CISCO_ROUTER_EVENT
Trigger description: Router device event to apply port configuration
Trigger environment: Parameters that can be set in the shell - $NATIVE_VLAN=(1)
 The value in the parenthesis is a default value
Trigger mapping function: CISCO_ROUTER_AUTO_SMARTPORT

Trigger Id: CISCO_SWITCH_ETHERCHANNEL_CONFIG
Trigger description: etherchannel parameter
Trigger environment: $INTERFACE_LIST=(),$PORT-CHANNEL_ID=(),
                              $EC_MODE=(),$EC_PROTOCOLTYPE=(),
                              PORT-CHANNEL_TYPE=()
Trigger mapping function: CISCO_ETHERCHANNEL_AUTOSMARTPORT

Trigger Id: CISCO_SWITCH_EVENT
Trigger description: Switch device event to apply port configuration
Trigger environment: Parameters that can be set in the shell - $NATIVE_VLAN=(1)
 The value in the parenthesis is a default value
Trigger mapping function: CISCO_SWITCH_AUTO_SMARTPORT

Trigger Id: CISCO_WIRELESS_AP_EVENT
Trigger description: Autonomous ap device event to apply port configuration
Trigger environment: Parameters that can be set in the shell - $NATIVE_VLAN=(1)
 The value in the parenthesis is a default value
Trigger mapping function: CISCO_AP_AUTO_SMARTPORT

Trigger Id: CISCO_WIRELESS_LIGHTWEIGHT_AP_EVENT
Trigger description: Lightweight-ap device event to apply port configuration
Trigger environment: Parameters that can be set in the shell - $ACCESS_VLAN=(1)
  The value in the parenthesis is a default value
Trigger mapping function: CISCO_LWAP_AUTO_SMARTPORT

Trigger Id: word
Trigger description: word
Trigger environment:
Trigger mapping function:
```

This example shows how to use the **show shell functions** command to view the built-in macros in the switch software:

```
Device# show shell functions
#User defined functions:

#Built-in functions:
function CISCO_AP_AUTO_SMARTPORT () {
    if [[ $LINKUP == YES ]]; then
        conf t
            interface  $INTERFACE
                macro description $TRIGGER
                switchport trunk encapsulation dot1q
                switchport trunk native vlan $NATIVE_VLAN
                switchport trunk allowed vlan ALL
```

```
                switchport mode trunk
                switchport nonegotiate
                auto qos voip trust
                mls qos trust cos
                if [[ $LIMIT == 0 ]]; then
                  default srr-queue bandwidth limit
                else
                  srr-queue bandwidth limit $LIMIT
                fi
                if [[ $SW_POE == YES ]]; then
                   if [[ $AP125X == AP125X ]]; then
                      macro description AP125X
                      macro auto port sticky
                      power inline port maximum 20000
                   fi
                fi
             exit
        end
    fi
    if [[ $LINKUP == NO ]]; then
        conf t
            interface  $INTERFACE
                no macro description
                no switchport nonegotiate
                no switchport trunk native vlan $NATIVE_VLAN
                no switchport trunk allowed vlan ALL
                no auto qos voip trust
                no mls qos trust cos
                default srr-queue bandwidth limit
                if [[ $AUTH_ENABLED == NO ]]; then
                  no switchport mode
                  no switchport trunk encapsulation
                fi
                if [[ $STICKY == YES ]]; then
                   if [[ $SW_POE == YES ]]; then
                      if [[ $AP125X == AP125X ]]; then
                         no macro auto port sticky
                         no power inline port maximum
                      fi
                   fi
                fi
            exit
        end
    fi
}
<output truncated>
```

show system mtu

To display the global maximum transmission unit (MTU) or maximum packet size set for the switch, use the **show system mtu** command in privileged EXEC mode.

show system mtu

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

For information about the MTU values and the stack configurations that affect the MTU values, see the **system mtu** command.

Examples

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

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

show tech-support

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

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

Syntax Description

cef	(Optional) Displays CEF related information.
cft	(Optional) Displays CFT related information.
eigrp	(Optional) Displays EIGRP related information.
evc	(Optional) Displays EVC related information.
fnf	(Optional) Displays flexible netflow related information.
ipc	(Optional) Displays IPC related information.
ipmulticast	(Optional) Displays IP multicast related information.
ipsec	(Optional) Displays IPSEC related information.
isis	(Optional) Displays CLNS and ISIS related information.
license	(Optional) Displays license related information.
lisp	(Optional) Displays Locator/ID Separation Protocol related information.
memory	(Optional) Displays Memory related information.
mfib	(Optional) Displays MFIB related information.
msrp	(Optional) Displays MSRP related information.
mvrp	(Optional) Displays MVRP related information.
nat	(Optional) Displays NAT related information.
onep	(Optional) Displays ONEP related information.
ospf	(Optional) Displays OSPF related information.
page	(Optional) Displays the command output on a single page at a time. Use the Return key to display the next line of output or use the space bar to display the next page of information. If not used, the output scrolls (that is, it does not stop for page breaks). Press the **Ctrl-C** keys to stop the command output.
password	(Optional) Leaves passwords and other security information in the output. If not used, passwords and other security-sensitive information in the output are replaced with the label "<removed>".

performance-monitor	(Optional) Displays Performance Monitor related information.
pki	(Optional) Displays PKI related information.
platform	(Optional) Displays Platform related information.
qos	(Optional) Displays QoS related information.
subscriber	(Optional) Displays subscriber related information.
switch-report	(Optional) Archives switch report.
vrrp	(Optional) Displays VRRP related information.
wccp	(Optional) Displays WCCP related information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was implemented.

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.

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.

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

Release	Modification
	This command was introduced.

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 automnatically 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

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

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**

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

speed {**10** | **100** | **1000** | **2500** | **5000** | **auto** [{**10** | **100** | **1000** | **2500** | **5000**}] | **nonegotiate**}
no speed

Syntax Description

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

Command Default

The default is **auto**.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

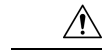
You cannot configure speed on 10-Gigabit Ethernet ports.

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

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

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



Caution Changing the interface speed and duplex mode configuration might shut down and re-enable the interface during the reconfiguration.

For guidelines on setting the switch speed and duplex parameters, see the "Configuring Interface Characteristics" chapter in the software configuration guide for this release.

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

Examples

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

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

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

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

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

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

start (coap-proxy configuration)

To start CoAP on the switch, use the **start** command in coap-proxy configuration mode.

start

Command Modes

coap-proxy configuration (config-coap-proxy)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

To access coap-proxy configuration mode, enter the **coap proxy** command in global configuration mode.

Example

This example shows how to start CoAP on the switch.

```
Device(config)# coap proxy
Device(config-coap-proxy)# start
```

stop (coap-proxy configuration)

To stop CoAP on the switch, use the **stop** command in coap-proxy configuration mode.

stop

Command Modes

coap-proxy configuration (config-coap-proxy)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

To access coap-proxy configuration mode, enter the **coap proxy** command in global configuration mode.

Example

This example shows how to stop CoAP on the switch.

```
Device(config)# coap proxy
Device(config-coap-proxy)# stop
```

switchport block

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

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

Syntax Description

multicast	Specifies that unknown multicast traffic should be blocked. **Note** Only pure Layer 2 multicast traffic is blocked. Multicast packets that contain IPv4 or IPv6 information in the header are not blocked.
unicast	Specifies that unknown unicast traffic should be blocked.

Command Default

Unknown multicast and unicast traffic is not blocked.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

By default, all traffic with unknown MAC addresses is sent to all ports. You can block unknown multicast or unicast traffic on protected or nonprotected ports. If unknown multicast or unicast traffic is not blocked on a protected port, there could be security issues.

With multicast traffic, the port blocking feature blocks only pure Layer 2 packets. Multicast packets that contain IPv4 or IPv6 information in the header are not blocked.

Blocking unknown multicast or unicast traffic is not automatically enabled on protected ports; you must explicitly configure it.

For more information about blocking packets, see the software configuration guide for this release.

This example shows how to block unknown unicast traffic on an interface:

```
Device(config-if)# switchport block unicast
```

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

system mtu

To set the global maximum packet size or MTU size for switched packets on Gigabit Ethernet and 10-Gigabit Ethernet ports, use the **system mtu** command in global configuration mode. To restore the global MTU value to its default value, use the **no** form of this command.

system mtu *bytes*
no system mtu

Syntax Description

bytes	The global MTU size in bytes. The range is 1500 to 9198 bytes; the default is 1500 bytes.

Command Default

The default MTU size for all ports is 1500 bytes.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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

The switch does not support the MTU on a per-interface basis.

If you enter a value that is outside the allowed range for the specific type of interface, the value is not accepted.

Examples

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

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

transport (coap-proxy configuration)

To configure transport protocol, use the **transport** command in coap-proxy configuration mode.

transport{**tcp** | **udp**}

Syntax Description

tcp	Specifies a TCP protocol.
udp	Specifies a UDP protocol.

Command Modes

coap-proxy configuration (config-coap-proxy)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

To access coap-proxy configuration mode, enter the **coap proxy** command in global configuration mode.

Example

This is an example to configure tcp as transport protocol

```
Device(config)# coap proxy
Device(config-coap-proxy)# transport tcp
```

voice-signaling vlan (network-policy configuration)

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

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

Syntax Description

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

Command Default

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

The default CoS value is 5.

The default DSCP value is 46.

The default tagging mode is untagged.

Command Modes

Network-policy profile configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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

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

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

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

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

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

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

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

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

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

voice vlan (network-policy configuration)

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

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

Syntax Description

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

Command Default

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

The default CoS value is 5.

The default DSCP value is 46.

The default tagging mode is untagged.

Command Modes

Network-policy profile configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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

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

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

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

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

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

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

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

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

PART IV

IP Addressing Services

• IP Addressing Services Commands, on page 349

IP Addressing Services Commands

- clear ipv6 access-list, on page 353
- clear ipv6 dhcp, on page 354
- clear ipv6 dhcp binding, on page 355
- clear ipv6 dhcp client, on page 356
- clear ipv6 dhcp conflict, on page 357
- clear ipv6 dhcp relay binding, on page 358
- clear ipv6 eigrp, on page 359
- clear ipv6 mfib counters, on page 360
- clear ipv6 mld counters, on page 361
- clear ipv6 mld traffic, on page 362
- clear ipv6 mtu, on page 363
- clear ipv6 multicast aaa authorization, on page 364
- clear ipv6 nd destination, on page 365
- clear ipv6 nd on-link prefix, on page 366
- clear ipv6 nd router, on page 367
- clear ipv6 neighbors, on page 368
- clear ipv6 ospf, on page 370
- clear ipv6 ospf counters, on page 371
- clear ipv6 ospf events, on page 373
- clear ipv6 pim reset, on page 374
- clear ipv6 pim topology, on page 375
- clear ipv6 pim traffic, on page 376
- clear ipv6 prefix-list, on page 377
- clear ipv6 rip, on page 378
- clear ipv6 route, on page 379
- clear ipv6 spd, on page 380
- fhrp delay, on page 381
- fhrp version vrrp v3, on page 382
- ip address dhcp, on page 383
- ip address pool (DHCP), on page 386
- ip address, on page 387
- ip unnumbered, on page 389
- ip wccp, on page 391

- ipv6 access-list, on page 396
- ipv6 address-validate, on page 399
- ipv6 cef, on page 400
- ipv6 cef accounting, on page 402
- ipv6 cef distributed, on page 404
- ipv6 cef load-sharing algorithm, on page 406
- ipv6 cef optimize neighbor resolution, on page 407
- ipv6 destination-guard policy, on page 408
- ipv6 dhcp-relay bulk-lease, on page 409
- ipv6 dhcp-relay option vpn, on page 410
- ipv6 dhcp-relay source-interface, on page 411
- ipv6 dhcp binding track ppp, on page 412
- ipv6 dhcp database, on page 413
- ipv6 dhcp iana-route-add, on page 415
- ipv6 dhcp iapd-route-add, on page 416
- **ipv6 dhcp-ldra** , on page 417
- ipv6 dhcp ping packets, on page 418
- ipv6 dhcp pool, on page 419
- ipv6 dhcp server vrf enable, on page 421
- ipv6 flow monitor , on page 422
- ipv6 general-prefix, on page 423
- ipv6 local policy route-map, on page 425
- ipv6 local pool, on page 427
- ipv6 mld snooping (global), on page 429
- ipv6 mld ssm-map enable, on page 430
- ipv6 mld state-limit, on page 431
- ipv6 multicast-routing, on page 432
- ipv6 multicast group-range, on page 433
- ipv6 multicast pim-passive-enable, on page 435
- ipv6 nd cache expire, on page 436
- ipv6 nd cache interface-limit (global), on page 437
- ipv6 nd host mode strict, on page 438
- ipv6 nd na glean, on page 439
- ipv6 nd ns-interval, on page 440
- ipv6 nd nud retry, on page 441
- ipv6 nd reachable-time, on page 443
- ipv6 nd resolution data limit, on page 444
- ipv6 nd route-owner, on page 445
- ipv6 neighbor, on page 446
- ipv6 ospf name-lookup, on page 448
- ipv6 pim, on page 449
- ipv6 pim accept-register, on page 450
- ipv6 pim allow-rp , on page 451
- ipv6 pim neighbor-filter list, on page 452
- ipv6 pim rp-address, on page 453
- ipv6 pim rp embedded, on page 456

- ipv6 pim spt-threshold infinity, on page 457
- ipv6 prefix-list, on page 458
- ipv6 source-guard attach-policy, on page 461
- ipv6 source-route, on page 462
- ipv6 spd mode, on page 464
- ipv6 spd queue max-threshold, on page 465
- ipv6 traffic interface-statistics, on page 466
- ipv6 unicast-routing, on page 467
- key chain, on page 468
- key-string (authentication), on page 469
- key, on page 470
- show ip ports all, on page 472
- show ipv6 access-list, on page 474
- show ipv6 destination-guard policy, on page 476
- show ipv6 dhcp, on page 477
- show ipv6 dhcp binding, on page 478
- show ipv6 dhcp conflict, on page 481
- show ipv6 dhcp database, on page 482
- show ipv6 dhcp guard policy, on page 484
- show ipv6 dhcp interface, on page 486
- show ipv6 dhcp relay binding, on page 488
- show ipv6 eigrp events, on page 490
- show ipv6 eigrp interfaces, on page 492
- show ipv6 eigrp topology, on page 494
- show ipv6 eigrp traffic, on page 496
- show ipv6 general-prefix, on page 498
- show ipv6 interface, on page 499
- show ipv6 mfib, on page 507
- show ipv6 mld groups, on page 513
- show ipv6 mld interface, on page 516
- show ipv6 mld snooping, on page 518
- show ipv6 mld ssm-map, on page 520
- show ipv6 mld traffic, on page 522
- show ipv6 mrib client, on page 524
- show ipv6 mrib route, on page 526
- show ipv6 mroute, on page 528
- show ipv6 mtu, on page 532
- show ipv6 nd destination, on page 534
- show ipv6 nd on-link prefix, on page 535
- show ipv6 neighbors, on page 536
- show ipv6 ospf, on page 540
- show ipv6 ospf border-routers, on page 544
- show ipv6 ospf event, on page 546
- show ipv6 ospf graceful-restart, on page 549
- show ipv6 ospf interface, on page 551
- show ipv6 ospf request-list, on page 556

- show ipv6 ospf retransmission-list, on page 558
- show ipv6 ospf statistics, on page 560
- show ipv6 ospf summary-prefix, on page 562
- show ipv6 ospf timers rate-limit, on page 563
- show ipv6 ospf traffic, on page 564
- show ipv6 ospf virtual-links, on page 568
- show ipv6 pim anycast-RP, on page 570
- show ipv6 pim bsr, on page 571
- show ipv6 pim df, on page 573
- show ipv6 pim group-map, on page 575
- show ipv6 pim interface, on page 577
- show ipv6 pim join-prune statistic, on page 579
- show ipv6 pim limit, on page 580
- show ipv6 pim neighbor, on page 581
- show ipv6 pim range-list, on page 583
- show ipv6 pim topology, on page 585
- show ipv6 pim traffic, on page 587
- show ipv6 pim tunnel, on page 589
- show ipv6 policy, on page 591
- show ipv6 prefix-list, on page 592
- show ipv6 protocols, on page 594
- show ipv6 rip, on page 596
- show ipv6 routers, on page 601
- show ipv6 rpf, on page 604
- show ipv6 source-guard policy, on page 606
- show ipv6 spd, on page 607
- show ipv6 static, on page 608
- show ipv6 traffic, on page 612
- show key chain, on page 615
- show track, on page 616
- track, on page 618
- vrrp, on page 620
- vrrp description, on page 621
- vrrp preempt, on page 622
- vrrp priority, on page 623
- vrrp timers advertise, on page 624
- vrrs leader, on page 626

clear ipv6 access-list

To reset the IPv6 access list match counters, use the **clear ipv6 access-list**command in privileged EXEC mode.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
# clear ipv6 access-list marketing
```

Related Commands

Command	Description
hardware statistics	Enables the collection of hardware statistics.
ipv6 access-list	Defines an IPv6 access list and enters IPv6 access list configuration mode.
show ipv6 access-list	Displays the contents of all current IPv6 access lists.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The **clear ipv6 dhcp** command deletes DHCP for IPv6 information.

Examples

The following example :

```
# 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

ipv6-address	(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.
vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
# clear ipv6 dhcp binding
```

Related Commands

Command	Description
show ipv6 dhcp binding	Displays automatic client bindings from the DHCP for IPv6 server binding 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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
# clear ipv6 dhcp client Ethernet 1/0
```

Related Commands

Command	Description
show ipv6 dhcp interface	Displays DHCP for IPv6 interface information.

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

*****	Clears all address conflicts.
ipv6-address	Clears the host IPv6 address that contains the conflicting address.
vrf *vrf-name*	Specifies a virtual routing and forwarding (VRF) name.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
# clear ipv6 dhcp conflict *
```

Related Commands

Command	Description
show ipv6 dhcp conflict	Displays address conflicts found by a DHCPv6 server when addresses are offered to the client.

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-addressipv6-prefix*}

clear ipv6 dhcp relay binding{**vrf** *vrf-name*}{** ipv6-prefix*}

Syntax Description

vrf *vrf-name*	Specifies a virtual routing and forwarding (VRF) configuration.
*	Clears all DHCPv6 relay bindings.
ipv6-address	DHCPv6 address.
ipv6-prefix	IPv6 prefix.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
# 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:

```
# clear ipv6 dhcp relay binding vrf vrf1 2001:DB8:0:1::/64
```

Related Commands

Command	Description
show ipv6 dhcp relay binding	Displays DHCPv6 IANA and DHCPv6 IAPD bindings on a relay agent.

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

as-number	(Optional) Autonomous system number.
neighbor	(Optional) Deletes neighbor router entries.
ipv6-address	(Optional) IPv6 address of a neighboring router.
interface-type	(Optional) The interface type of the neighbor router.
interface-number	(Optional) The interface number of the neighbor router.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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-typeinterface-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:

```
# 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-addresssource-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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
# 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

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
interface-type	(Optional) Interface type. For more information, use the question mark (**?**) online help function.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
# clear ipv6 mld counters Ethernet1/0
```

Related Commands

Command	Description
show ipv6 mld interface	Displays multicast-related information about an interface.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Using the **clear ipv6 mld traffic** command will reset all MLD traffic counters.

Examples

The following example resets the MLD traffic counters:

```
# clear ipv6 mld traffic
```

Command	Description
show ipv6 mld traffic	Displays the MLD traffic counters.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

If a router is flooded with ICMPv6 toobig 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:

```
# clear ipv6 mtu
```

Related Commands

Command	Description
ipv6 flowset	Configures flow-label marking in 1280-byte or larger packets sent by the router.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
# clear ipv6 multicast aaa authorization FastEthernet 1/0
```

Related Commands

Command	Description
aaa authorization multicast default	Sets parameters that restrict user access to an IPv6 multicast network.

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

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
# clear ipv6 nd destination
```

Related Commands

Command	Description
ipv6 nd host mode strict	Enables the conformant, or strict, IPv6 host mode.

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

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
# clear ipv6 nd on-link prefix
```

Related Commands

Command	Description
ipv6 nd host mode strict	Enables the conformant, or strict, IPv6 host mode.

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

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
# clear ipv6 nd router
```

Related Commands

Command	Description
ipv6 nd host mode strict	Enables the conformant, or strict, IPv6 host mode.

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**}]}]

clear ipv6 neighbors

Syntax Description

interface *type number*	(Optional) Clears the IPv6 neighbor discovery cache in the specified interface.
ipv6 *ipv6-address*	(Optional) Clears the IPv6 neighbor discovery cache that matches the specified IPv6 address on the specified interface.
statistics	(Optional) Clears the IPv6 neighbor discovery entry cache.
vrf	(Optional) Clears entries for a virtual private network (VPN) routing or forwarding instance.
table-name	(Optional) Table name or identifier. The value range is from 0x0 to 0xFFFFFFFF (0 to 65535 in decimal).

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The **clear ipv6 neighbor** 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:

```
# 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:

```
# 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:

```
# clear ipv6 neighbors interface Ethernet0/0 ipv6 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.

```
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

Command	Description
ipv6 neighbor	Configures a static entry in the IPv6 neighbor discovery cache.
show ipv6 neighbors	Displays IPv6 neighbor discovery cache information.

clear ipv6 ospf

To clear the Open Shortest Path First (OSPF) state based on the OSPF routing process ID, use the **cl ear ipv6 ospf** command in privileged EXEC mode.

clear ipv6 ospf [*process-id*] {**process** | **force-spf** | **redistribution**}

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.
process	Restarts the OSPF process.
force-spf	Starts the shortest path first (SPF) algorithm without first clearing the OSPF database.
redistribution	Clears OSPF route redistribution.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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 OSPFprocess. If the *process-id*optionis not specified,all OSPF processesare cleared.

Examples

The following example starts the SPF algorithm without clearing the OSPF database:

```
# 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 **cl ear 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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
# 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:

```
# 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:

```
# 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

Command	Description
show ipv6 ospf neighbor	Displays OSPF neighbor information on a per-interface basis.

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 **cl ear 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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
# 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

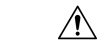
Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
# 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-namegroup-address*}]

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.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

This command clears PIM protocol informationfrom 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:

```
# 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

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
# 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

prefix-list-name	(Optional) The name of the prefix list from which the hit count is to be cleared.
ipv6-prefix	(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.
/ *prefix-length*	(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.

Command Default

The hit count is automatically cleared for all IPv6 prefix lists.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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.

```
# clear ipv6 prefix-list first_list 2001:0DB8::/35
```

Related Commands

Command	Description
ipv6 prefix-list	Creates an entry in an IPv6 prefix list.
ipv6 prefix-list sequence-number	Enables the generation of sequence numbers for entries in an IPv6 prefix list.
show ipv6 prefix-list	Displays information about an IPv6 prefix list or prefix list entries.

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*]

clear ipv6 rip [*name*]

Syntax Description

name	(Optional) Name of an IPv6 RIP process.
vrf *vrf-name*	(Optional) Clears information about the specified Virtual Routing and Forwarding (VRF) instance.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
# clear ipv6 rip one
```

The following example deletes the IPv6 VRF instance, called vrf1 for the RIP process, called one:

```
# clear ipv6 rip one vrf vrf1

*Mar 15 12:36:17.022: RIPng: Deleting 2001:DB8::/32
*Mar 15 12:36:17.022: [Exec]IPv6RT[vrf1]: rip <name>, Delete all next-hops for 2001:DB8::1
*Mar 15 12:36:17.022: [Exec]IPv6RT[vrf1]: rip <name>, Delete 2001:DB8::1 from table
*Mar 15 12:36:17.022: [IPv6 RIB Event Handler]IPv6RT[<red>]: Event: 2001:DB8::1, Del, owner
 rip, previous None
```

Related Commands

Command	Description
debug ipv6 rip	Displays the current contents of the IPv6 RIP routing table.
ipv6 rip vrf-mode enable	Enables VRF-aware support for IPv6 RIP.
show ipv6 rip	Displays the current content of the IPv6 RIP routing 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-addressipv6-prefix/prefix-length*} | *****}

Syntax Description

ipv6-address	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.
ipv6-prefix	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.
/ *prefix-length*	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.
*****	Clears all IPv6 routes.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
# clear ipv6 route 2001:0DB8::/35
```

Related Commands

Command	Description
ipv6 route	Establishes static IPv6 routes.
show ipv6 route	Displays the current contents of the IPv6 routing 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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
# clear ipv6 spd
```

fhrp delay

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

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

Syntax Description

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

Command Default

None

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Examples

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

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

Related Commands

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

fhrp version vrrp v3

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

fhrp version vrrp v3
no fhrp version vrrp v3

Syntax Description

This command has no keywords or arguments.

Command Default

VRRPv3 and VRRS configuration on a device is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

When VRRPv3 is in use, VRRP version 2 (VRRPv2) is unavailable.

Examples

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

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

Related Commands

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

ip address dhcp

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

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

Syntax Description

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

Command Default

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

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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 aa15snap encapsulation type.

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

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

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

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

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

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

Table 26: Configuration Method and Resulting Contents of the DISCOVER Message

Configuration Method	Contents of DISCOVER Messages
ip address dhcp	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.
ip address dhcp hostname *hostname*	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.
ip address dhcp client-id ethernet 1	The DISCOVER message contains the MAC address of the Ethernet 1 interface in the client ID field and contains the default hostname of the device in the option 12 field.
ip address dhcp client-id ethernet 1 hostname *hostname*	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.

Examples

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

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

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

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

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

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

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

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

Related Commands

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

ip address pool (DHCP)

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

ip address pool *name*
no ip address pool

Syntax Description

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

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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

Examples

The following example specifies that the IP address of GigabitEthernet interface 1/0/1 will be automatically configured from the address pool named abc:

```
ip dhcp pool abc
  import all
  origin ipcp
!
interface GigabitEthernet 1/0/1
  ip address pool abc
```

Related Commands

Command	Description
show ip interface	Displays the usability status of interfaces configured for IP.

ip address

To set a primary or secondary IP address for an interface, use the **ip address** command in interface configuration mode. To remove an IP address or disable IP processing, use the noform of this command.

ip address *ip-address mask* [**secondary** [**vrf** *vrf-name*]]
no ip address *ip-address mask* [**secondary** [**vrf** *vrf-name*]]

Syntax Description

ip-address	IP address.
mask	Mask for the associated IP subnet.
secondary	(Optional) Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address. **Note** If the secondary address is used for a VRF table configuration with the **vrf** keyword, the **vrf** keyword must be specified also.
vrf	(Optional) Name of the VRF table. The *vrf-name* argument specifies the VRF name of the ingress interface.

Command Default

No IP address is defined for the interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

An interface can have one primary IP address and multiple secondary IP addresses. Packets generated by the Cisco IOS software always use the primary IP address. Therefore, all devices and access servers on a segment should share the same primary network number.

Hosts can determine subnet masks using the Internet Control Message Protocol (ICMP) mask request message. Devices respond to this request with an ICMP mask reply message.

You can disable IP processing on a particular interface by removing its IP address with the **no ip address** command. If the software detects another host using one of its IP addresses, it will print an error message on the console.

The optional **secondary** keyword allows you to specify an unlimited number of secondary addresses. Secondary addresses are treated like primary addresses, except the system never generates datagrams other than routing updates with secondary source addresses. IP broadcasts and Address Resolution Protocol (ARP) requests are handled properly, as are interface routes in the IP routing table.

Secondary IP addresses can be used in a variety of situations. The following are the most common applications:

- There may not be enough host addresses for a particular network segment. For example, your subnetting allows up to 254 hosts per logical subnet, but on one physical subnet you need 300 host addresses. Using

secondary IP addresses on the devices or access servers allows you to have two logical subnets using one physical subnet.

- Many older networks were built using Level 2 bridges. The judicious use of secondary addresses can aid in the transition to a subnetted, device-based network. Devices on an older, bridged segment can be easily made aware that many subnets are on that segment.
- Two subnets of a single network might otherwise be separated by another network. This situation is not permitted when subnets are in use. In these instances, the first network is *extended*, or layered on top of the second network using secondary addresses.

Note

- If any device on a network segment uses a secondary address, all other devices on that same segment must also use a secondary address from the same network or subnet. Inconsistent use of secondary addresses on a network segment can very quickly cause routing loops.
- 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.
- If you configure a secondary IP address, you must disable sending ICMP redirect messages by entering the **no ip redirects** command, to avoid high CPU utilization.

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:

```
Device> enable
Device# configure terminal
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# ip address 192.108.1.27 255.255.255.0
Device(config-if)# ip address 192.31.7.17 255.255.255.0 secondary
```

Related Commands

Command	Description
match ip route-source	Specifies a source IP address to match to required route maps that have been set up based on VRF connected routes.
route-map	Defines the conditions for redistributing routes from one routing protocol into another, or to enable policy routing.
set vrf	Enables VPN VRF selection within a route map for policy-based routing VRF selection.
show ip arp	Displays the ARP cache, in which SLIP addresses appear as permanent ARP table entries.
show ip interface	Displays the usability status of interfaces configured for IP.
show route-map	Displays static and dynamic route maps.

ip unnumbered

To enable IP processing on an interface without assigning an explicit IP address to the interface, use the **ip unnumbered** command in interface configuration mode or subinterface configuration mode. To disable the IP processing on the interface, use the **no** form of this command.

ip unnumbered *type number* [**poll**] [**point-to-point**]
no ip unnumbered [*type number*]

Syntax Description

type	Type of interface. For more information, use the question mark (**?**) online help function.
number	Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (**?**) online help function.
poll	(Optional) Enables IP connected host polling.
point-to-point	(Optional) Enables point to point connection.

Command Default

Unnumbered interfaces are not supported.

Command Modes

Interface configuration (config-if)

Subinterface configuration (config-subif)

Command History

Release	Modification
Cisco IOS XE Fuji 16.8.1a	This command was introduced.

Usage Guidelines

When an unnumbered interface generates a packet (for example, for a routing update), it uses the address of the specified interface as the source address of the IP packet. It also uses the address of the specified interface in determining which routing processes are sending updates over the unnumbered interface.

The following restrictions are applicable for this command:

- Serial interfaces using High-Level Data Link Control (HDLC), PPP, Link Access Procedure Balanced (LAPB), Frame Relay encapsulations, and Serial Line Internet Protocol (SLIP), and tunnel interfaces can be unnumbered.
- You cannot use the **ping** EXEC command to determine whether the interface is up because the interface has no address. Simple Network Management Protocol (SNMP) can be used to remotely monitor interface status.
- It is not possible to netboot a Cisco IOS image over a serial interface that is assigned an IP address with the **ip unnumbered** command.
- You cannot support IP security options on an unnumbered interface.

The interface that you specify using the *type* and *number* arguments must be enabled (listed as “up” in the **show interfaces** command display).

If you are configuring Intermediate System-to-Intermediate System (IS-IS) across a serial line, you must configure the serial interfaces as unnumbered. This configuration allows you to comply with RFC 1195, which states that IP addresses are not required on each interface.

Note Using an unnumbered serial line between different major networks (or *majornets*) requires special care. If at each end of the link there are different majornets assigned to the interfaces that you specified as unnumbered, any routing protocol that is running across the serial line must not advertise subnet information.

Examples

The following example shows how to assign the address of Ethernet 0 to the first serial interface:

```
Device(config)# interface ethernet 0
Device(config-if)# ip address 10.108.6.6 255.255.255.0
!
Device(config-if)# interface serial 0
Device(config-if)# ip unnumbered ethernet 0
```

The following example shows how to configure Ethernet VLAN subinterface 3/0.2 as an IP unnumbered subinterface:

```
Device(config)# interface ethernet 3/0.2
Device(config-subif)# encapsulation dot1q 200
Device(config-subif)# ip unnumbered ethernet 3/1
```

The following example shows how to configure Fast Ethernet subinterfaces in the range from 5/1.1 to 5/1.4 as IP unnumbered subinterfaces:

```
Device(config)# interface range fastethernet5/1.1 - fastethernet5/1.4
Device(config-if-range)# ip unnumbered ethernet 3/1
```

The following example shows how to enable polling on a Gigabit Ethernet interface:

```
Device(config)# interface loopback0
Device(config-if)# ip address 10.108.6.6 255.255.255.0
!
Device(config-if)# ip unnumbered gigabitethernet 3/1
Device(config-if)# ip unnumbered loopback0 poll
```

ip wccp

To enable support of the specified Web Cache Communication Protocol (WCCP) service for participation in a service group, use the **ip wccp** command in global configuration mode. To disable the service group, use the **no** form of this command.

ip wccp [{ **vrf** *vrf-name* }] { **web-cache** *service-number* } [**service-list** *service-access-list*] [**mode** { **open** | **closed** }] [**group-address** *multicast-address*] [**redirect-list** *access-list*] [**group-list** *access-list*] [**password** [{ **0** | **7** }] *password*]
no ip wccp [{ **vrf** *vrf-name* }] { **web-cache** *service-number* } [**service-list** *service-access-list*] [**mode** { **open** | **closed** }] [**group-address** *multicast-address*] [**redirect-list** *access-list*] [**group-list** *access-list*] [**password** [{ **0** | **7** }] *password*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding instance (VRF) to associate with a service group.
web-cache	Specifies the web-cache service (WCCP Version 1 and Version 2). **Note** Web-cache counts as one of the services. The maximum number of services, including those assigned with the *service-number* argument, is 256.
service-number	Dynamic service identifier, which means the service definition is dictated by the cache. The dynamic service number can be from 0 to 254. The maximum number of services is 256, which includes the web-cache service specified with the **web-cache** keyword. **Note** If Cisco cache engines are used in the cache cluster, the reverse proxy service is indicated by a value of 99.
service-list *service-access-list*	(Optional) Identifies a named extended IP access list that defines the packets that will match the service.
mode open	(Optional) Identifies the service as open. This is the default service mode.
mode closed	(Optional) Identifies the service as closed.
group-address *multicast-address*	(Optional) Specifies the multicast IP address that communicates with the WCCP service group. The multicast address is used by the device to determine which web cache should receive redirected messages.
redirect-list *access-list*	(Optional) Specifies the access list that controls traffic redirected to this service group. The *access-list* argument should consist of a string of no more than 64 characters (name or number) in length that specifies the access list.
group-list *access-list*	(Optional) Specifies the access list that determines which web caches are allowed to participate in the service group. The *access-list* argument specifies either the number or the name of a standard or extended access list.

password [**0** | **7**] *password*	(Optional) Specifies the message digest algorithm 5 (MD5) authentication for messages received from the service group. Messages that are not accepted by the authentication are discarded. The encryption type can be 0 or 7, with 0 specifying not yet encrypted and 7 for proprietary. The *password* argument can be up to eight characters in length.

Command Default

WCCP services are not enabled on the device.

Command Modes

Global configuration (config)

Command History

Release	Modification
	This command was introduced.
Cisco IOS XE Bengaluru 17.6.1	The **vrf** keyword and *vrf-name* argument pair were added.

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 device 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 device can participate in the establishment of a service group.

Note All WCCP parameters must be included in a single IP WCCP command. For example: **ip wccp 61 redirect-list 10 password password**.

The **vrf** *vrf-name* keyword and argument pair is optional. It allows you to specify a VRF to associate with a service group. You can then specify a web-cache service name or service number.

The same service (web-cache or service number) can be configured in different VRF tables. Each service will operate independently.

When the **no ip wccp** command is entered, the device terminates participation in the service group, deallocates space if none of the interfaces still has 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. The following sections outline the specific usage of each of the optional forms of this command.

ip wccp [**vrf** *vrf-name*] {**web-cache** | *service-number*} **group-address** *multicast-address*

A WCCP group address can be configured to set up a multicast address that cooperating devices and web caches can use to exchange WCCP protocol messages. If such an address is used, IP multicast routing must be enabled so that the messages that use the configured group (multicast) addresses are received correctly.

This option instructs the device to use the specified multicast IP address to coalesce the "I See You" responses for the "Here I Am" messages that it has received on this group address. The response is also sent to the group address. The default is for no group address to be configured, in which case all "Here I Am" messages are responded to with a unicast reply.

ip wccp [**vrf** *vrf-name*] {**web-cache** | *service-number*} **redirect-list** *access-list*

This option instructs the device to use an access list to control the traffic that is redirected to the web caches of the service group specified by the service name given. The *access-list* argument specifies either the number or the name of a standard or extended access list. The access list itself specifies which traffic is permitted to be redirected. The default is for no redirect list to be configured (all traffic is redirected).

WCCP requires that the following protocol and ports not be filtered by any access lists:

- UDP (protocol type 17) port 2048. This port is used for control signaling. Blocking this type of traffic prevents WCCP from establishing a connection between the device and web caches.
- Generic routing encapsulation (GRE) (protocol type 47 encapsulated frames). Blocking this type of traffic prevents the web caches from ever seeing the packets that are intercepted.

ip wccp [**vrf** *vrf-name*] {**web-cache** | *service-number*} **group-list** *access-list*

This option instructs the device to use an access list to control the web caches that are allowed to participate in the specified service group. The *access-list* argument specifies either the number of a standard or extended access list or the name of any type of named access list. The access list itself specifies which web caches are permitted to participate in the service group. The default is for no group list to be configured, in which case all web caches may participate in the service group.

Note The **ip wccp** {**web-cache** | *service-number*} **group-list** command syntax resembles the **ip wccp** {**web-cache** | *service-number*} **group-listen** command, but these are entirely different commands. The **ip wccp group-listen** command is an interface configuration command used to configure an interface to listen for multicast notifications from a cache cluster.

ip wccp [**vrf** *vrf-name*] **web-cache** | *service-number*} **password** *password*

This option instructs the device to use MD5 authentication on the messages received from the service group specified by the service name given. Use this form of the command to set the password on the device. You must also configure the same password separately on each web cache. The password can be up to a maximum of eight characters in length. Messages that do not authenticate when authentication is enabled on the device are discarded. The default is for no authentication password to be configured and for authentication to be disabled.

ip wccp *service-number* **service-list** *service-access-list* **mode closed**

In applications where the interception and redirection of WCCP packets to external intermediate devices for the purpose of applying feature processing are not available within Cisco IOS software, packets for the application must be blocked when the intermediary device is not available. This blocking is called a closed service. By default, WCCP operates as an open service, wherein communication between clients and servers proceeds normally in the absence of an intermediary device. The **service-list** keyword can be used only for closed mode services. When a WCCP service is configured as closed, WCCP discards packets that do not have a client application registered to receive the traffic. Use the **service-list** keyword and *service-access-list* argument to register an application protocol type or port number.

When the definition of a service in a service list conflicts with the definition received via the WCCP protocol, a warning message similar to the following is displayed:

```
Sep 28 14:06:35.923: %WCCP-5-SERVICEMISMATCH: Service 90 mismatched on WCCP client 10.1.1.13
```

When there is service list definitions conflict, the configured definition takes precedence over the external definition received via WCCP protocol messages.

Examples

The following example shows how to configure a device to run WCCP reverse-proxy service, using the multicast address of 239.0.0.0:

```
Device> enable
Device# configure terminal
Device(config)# ip multicast-routing
Device(config)# ip wccp 99 group-address 239.0.0.0
Device(config)# interface ethernet 0
Device(config-if)# ip wccp 99 group-listen
```

The following example shows how to configure a device to redirect web-related packets without a destination of 10.168.196.51 to the web cache:

```
Device> enable
Device# configure terminal
Device(config)# access-list 100 deny ip any host 10.168.196.51
Device(config)# access-list 100 permit ip any any
Device(config)# ip wccp web-cache redirect-list 100
Device(config)# interface ethernet 0
Device(config-if)# ip wccp web-cache redirect out
```

The following example shows how to configure an access list to prevent traffic from network 10.0.0.0 leaving Fast Ethernet interface 0/0. Because the outbound access control list (ACL) check is enabled, WCCP does not redirect that traffic. WCCP checks packets against the ACL before they are redirected.

```
Device> enable
Device# configure terminal
Device(config)# ip wccp web-cache
Device(config)# ip wccp check acl outbound
Device(config)# interface fastethernet0/0
Device(config-if)# ip access-group 10 out
Device(config-if)# ip wccp web-cache redirect out
Device(config-if)# access-list 10 deny 10.0.0.0 0.255.255.255
Device(config-if)# access-list 10 permit any
```

If the outbound ACL check is disabled, HTTP packets from network 10.0.0.0 would be redirected to a cache, and users with that network address could retrieve web pages when the network administrator wanted to prevent this from happening.

The following example shows how to configure a closed WCCP service:

```
Device> enable
Device# configure terminal
Device(config)# ip wccp 99 service-list access1 mode closed
```

Note

- If multiple parameters are required, all parameters under **ip wccp** [**vrf** *vrf-name*] **web-cache** | *service-number*} must be configured as a single command.
- If the command is reissued with different parameters, the existing parameter will be removed and the new parameter will be configured.

The following example shows how to configure multiple parameters as a single command:

```
Device> enable
Device# configure terminal
Device(config)# ip wccp 61 group-address 10.0.0.1 password 0 password mode closed
redirect-list 121
```

Related Commands

Command	Description
ip wccp check services all	Enables all WCCP services.
ip wccp group listen	Configures an interface on a device to enable or disable the reception of IP multicast packets for WCCP.
ip wccp redirect exclude in	Enables redirection exclusion on an interface.
ip wccp redirect out	Configures redirection on an interface in the outgoing direction.
ip wccp version	Specifies which version of WCCP you want to use on your device.
show ip wccp	Displays global statistics related to WCCP.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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.

Note 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

Command	Description
deny (IPv6)	Sets deny conditions for an IPv6 access list.
ipv6 access-class	Filters incoming and outgoing connections to and from the device based on an IPv6 access list.
ipv6 pim bsr candidate rp	Configures the candidate RP to send PIM RP advertisements to the BSR.
ipv6 pim rp-address	Configure the address of a PIM RP for a particular group range.
ipv6 traffic-filter	Filters incoming or outgoing IPv6 traffic on an interface.
permit (IPv6)	Sets permit conditions for an IPv6 access list.
show ipv6 access-list	Displays the contents of all current IPv6 access lists.

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

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

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.

You must enter a minimum of eight characters of the **ipv6-address validate** command if you're using CLI help (?) for completing the syntax of this command. If you enter less than eight characters the command will conflict with the **no ipv6 address** command in interface configuration mode.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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 .

```
(config)# ip cef
(config)# ipv6 cef
```

Related Commands

Command	Description
ip route-cache	Controls the use of high-speed switching caches for IP routing.
ipv6 cef accounting	Enables Cisco Express Forwarding for IPv6 and distributed Cisco Express Forwarding for IPv6 network accounting.
ipv6 cef distributed	Enables distributed Cisco Express Forwarding for IPv6.
show cef	Displays which packets the line cards dropped or displays which packets were not express-forwarded.
show ipv6 cef	Displays entries in the IPv6 FIB.

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**}

Syntax Description

accounting-types	The *accounting-types* 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. • **load-balance-hash** --Enables load balancing hash bucket counters. • **non-recursive** --Enables accounting through nonrecursive prefixes. • **per-prefix** --Enables express forwarding of the collection of the number of packets and bytes to a destination (or prefix). • **prefix-length** --Enables accounting through prefix length.
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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
(config)# ipv6 cef accounting non-recursive
```

Related Commands

Command	Description
ip cef accounting	Enable Cisco Express Forwarding network accounting (for IPv4).
show cef	Displays information about packets **forwarded by Cisco Express Forwarding.**
show ipv6 cef	Displays entries in the IPv6 FIB.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
(config)# ipv6 cef distributed
```

Related Commands

Command	Description
ip route-cache	Controls the use of high-speed switching caches for IP routing.
show ipv6 cef	Displays entries in the IPv6 FIB.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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

Command	Description
ip cef load-sharing algorithm	Selects a Cisco Express Forwarding load-balancing algorithm (for IPv4).

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
(config)# ipv6 cef optimize neighbor resolution
```

Related Commands

Command	Description
ip cef optimize neighbor resolution	Configures address resolution optimization from Cisco Express Forwarding for IPv4 for directly connected neighbors.

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*]

Syntax Description

policy-name	(Optional) Name of the destination guard policy.

Command Default

No destination guard policy is defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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.

Examples

The following example shows how to define the name of a destination guard policy:

```
(config)#ipv6 destination-guard policy policy1
```

Related Commands

Command	Description
show ipv6 destination-guard policy	Displays destination guard information.

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

data-timeout	(Optional) Bulk lease query data transfer timeout.
seconds	(Optional) The range is from 60 seconds to 600 seconds. The default is 300 seconds.
retry	(Optional) Sets the bulk lease query retries.
number	(Optional) The range is from 0 to 5. The default is 5.
disable	(Optional) Disables the DHCPv6 bulk lease query feature.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
(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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
(config)# ipv6 dhcp-relay option vpn
```

Related Commands

Command	Description
ipv6 dhcp relay option vpn	Enables the DHCPv6 relay VRF-aware feature on an interface.

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

interface-type *interface-number*	(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.

Command Default

The address of the server-facing interface is used as the IPv6 relay source.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
(config)# ipv6 dhcp-relay source-interface loopback 0
```

Related Commands

Command	Description
ipv6 dhcp relay source-interface	Enables DHCP for IPv6 service on an interface.

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.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
(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*] `abort` [**timeout** *seconds*]
no ipv6 dhcp database *agent*

Syntax Description

agent	A flash, local bootflash, compact flash, NVRAM, FTP, TFTP, or Remote Copy Protocol (RCP) uniform resource locator.
write-delay *seconds*	(Optional) How often (in seconds) DHCP for IPv6 sends database updates. The default is 300 seconds. The minimum write delay is 60 seconds.
timeout *seconds*	(Optional) How long, in seconds, the router waits for a database transfer.

Command Default

Write-delay default is 300 seconds. Timeout default is 300 seconds.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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 canceled. By default, the DHCP for IPv6 server waits 300 seconds before canceling 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:

```
(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:

```
(config)# ipv6 dhcp database bootflash
```

Related Commands

Command	Description
clear ipv6 dhcp binding	Deletes automatic client bindings from the DHCP for IPv6 server binding table
show ipv6 dhcp database	Displays DHCP for IPv6 binding database agent information.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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

enable	Enables LDRA functionality on an access node.
disable	Disables LDRA functionality on an access node.

Command Default

By default, LDRA functionality is not enabled on an access node.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
(config)# ipv6 dhcp-ldra enable
(config)# exit
```

Note In the above example, Device denotes an access node.

Related Commands

Command	Description
ipv6 dhcp ldra attach-policy	Enables LDRA functionality on a VLAN.
ipv6 dhcp-ldra attach-policy	Enables LDRA functionality on an interface.

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*
ipv6 dhcp ping packets

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
(config)# ipv6 dhcp ping packets 4
```

Related Commands

Command	Description
clear ipv6 dhcp conflict	Clears an address conflict from the DHCPv6 server database.
show ipv6 dhcp conflict	Displays address conflicts found by a DHCPv6 server, or reported through a DECLINE message from a client.

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*

Syntax Description

poolname	User-defined name for the local prefix pool. The pool name can be a symbolic string (such as "Engineering") or an integer (such as 0).

Command Default

DHCP for IPv6 pools are not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
(config)# ipv6 dhcp pool cisco1
(config-dhcpv6)#
```

The following example shows how to configure an IPv6 address prefix for the IPv6 configuration pool cisco1:

```
(config-dhcpv6)# address prefix 2001:1000::0/64
(config-dhcpv6)# end
```

The following example shows how to configure a pool named engineering with three link-address prefixes and an IPv6 address prefix:

```
# configure terminal
(config)# ipv6 dhcp pool engineering
(config-dhcpv6)# link-address 2001:1001::0/64(config-dhcpv6)# link-address
2001:1002::0/64(config-dhcpv6)# link-address 2001:2000::0/48(config-dhcpv6)# address prefix
 2001:1003::0/64
(config-dhcpv6)# end
```

The following example shows how to configure a pool named 350 with vendor-specific options:

```
# configure terminal
(config)# ipv6 dhcp pool 350
(config-dhcpv6)# vendor-specific 9
(config-dhcpv6-vs)# suboption 1 address 1000:235D::1(config-dhcpv6-vs)# suboption 2 ascii
"IP-Phone"
(config-dhcpv6-vs)# end
```

Related Commands

Command	Description
ipv6 dhcp server	Enables DHCP for IPv6 service on an interface.
show ipv6 dhcp pool	Displays DHCP for IPv6 configuration pool information.

ipv6 dhcp server vrf enable

To enable the DHCP for IPv6 server VRF-aware feature, use the **ipv6 dhcp server vrf enable** command in global configuration mode. To disable the feature, use the **no** form of this command.

ipv6 dhcp server vrf enable
no ipv6 dhcp server vrf enable

Syntax Description

This command has no arguments or keywords.

Command Default

The DHCPv6 server VRF-aware feature is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The **ipv6 dhcp server option vpn** command allows the DHCPv6 server VRF-aware feature to be enabled globally on a device.

Examples

The following example enables the DHCPv6 server VRF-aware feature globally on a device:

```
(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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

You cannot attach a NetFlow monitor to a port channel interface. If both service module interfaces are part of an EtherChannel, you should attach the monitor to both physical interfaces.

This example shows how to apply a flow monitor to an interface:

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

prefix-name	The name assigned to the prefix.
ipv6-prefix	The IPv6 network assigned to the general prefix. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons. When defining a general prefix manually, specify both the *ipv6-prefix* and / *prefix-length* arguments.
/ *prefix-length*	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. When defining a general prefix manually, specify both the *ipv6-prefix* and / *prefix-length* arguments.
6to4	Allows configuration of a general prefix based on an interface used for 6to4 tunneling. When defining a general prefix based on a 6to4 interface, specify the **6to4** keyword and the *interface-type interface-number*argument.
interface-type interface-number	Interface type and number. For more information, use the question mark (**?**) online help function. When defining a general prefix based on a 6to4 interface, specify the **6to4** keyword and the *interface-type interface-number*argument.
6rd	Allows configuration of a general prefix computed from an interface used for IPv6 rapid deployment (6RD) tunneling.

Command Default

No general prefix is defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
(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:

```
(config)# ipv6 general-prefix my-prefix 6to4 ethernet0
```

Related Commands

Command	Description
show ipv6 general-prefix	Displays information on general prefixes for an IPv6 addresses.

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

route-map-name	Name of the route map to be used for local IPv6 PBR. The name must match a *route-map-name* value specified by the **route-map** command.

Command Default

IPv6 packets are not policy routed.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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

Command	Description
ipv6 policy route-map	Configures IPv6 PBR on an interface.
match ipv6 address	Specifies an IPv6 access list to be used to match packets for PBR for IPv6.
match length	Bases policy routing on the Level 3 length of a packet.

Command	Description
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set default interface	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.
set interface	Specifies the default interface to output packets that pass a match clause of a route map for policy routing.
set ipv6 default next-hop	Specifies an IPv6 default next hop to which matching packets will be forwarded.
set ipv6 next-hop (PBR)	Indicates where to output IPv6 packets that pass a match clause of a route map for policy routing.
set ipv6 precedence	Sets the precedence value in the IPv6 packet header.

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.

ipv6 local pool poolname prefix/prefix-length assigned-length [**shared**] [**cache-size** *size*]
no ipv6 local pool poolname

Syntax Description

poolname	User-defined name for the local prefix pool.
prefix	IPv6 prefix assigned to the pool. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
/ *prefix-length*	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).
assigned-length	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.
shared	(Optional) Indicates that the pool is a shared pool.
cache-size *size*	(Optional) Specifies the size of the cache.

Command Default

No pool is configured.

Command Modes

Global configuration (global)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
(config)# ipv6 local pool pool1 2001:0DB8::/29 64
(config)# end
# show ipv6 local pool
```

```
Pool Prefix Free In use
pool1  2001:0DB8::/29  65516  20
```

Related Commands

Command	Description
debug ipv6 pool	Enables IPv6 pool debugging.
peer default ipv6 address pool	Specifies the pool from which client prefixes are assigned for PPP links.
prefix-delegation pool	Specifies a named IPv6 local prefix pool from which prefixes are delegated to DHCP for IPv6 clients.
show ipv6 local pool	Displays information about any defined IPv6 address pools.

ipv6 mld snooping (global)

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced on the Supervisor Engine 720.

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:

```
(config)# ipv6 mld snooping
```

Related Commands

Command	Description
show ipv6 mld snooping	Displays MLDv2 snooping information.

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

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.

Command Default

The SSM mapping feature is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
(config)# ipv6 mld ssm-map enable
```

Related Commands

Command	Description
debug ipv6 mld ssm-map	Displays debug messages for SSM mapping.
ipv6 mld ssm-map query dns	Enables DNS-based SSM mapping.
ipv6 mld ssm-map static	Configures static SSM mappings.
show ipv6 mld ssm-map	Displays SSM mapping information.

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

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
number	Maximum number of MLD states allowed on a router. The valid range is from 1 to 64000.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
(config)# ipv6 mld state-limit 300
```

Related Commands

Command	Description
ipv6 mld access-group	Enables the performance of IPv6 multicast receiver access control.
ipv6 mld limit	Limits the number of MLD states resulting from MLD membership state on a per-interface basis.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
(config)# ipv6 multicast-routing
```

Related Commands

Command	Description
ipv6 pim rp-address	Configures the address of a PIM RP for a particular group range.
no ipv6 pim	Turns off IPv6 PIM on a specified interface.
no ipv6 mld router	Disables MLD router-side processing on a specified interface.

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

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
access-list-name	(Optional) Name of an access list that contains authenticated subscriber groups and authorized channels that can send traffic to the router.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
(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:

```
(config)# interface int2
(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

Command	Description
ipv6 mld access-group	Performs IPv6 multicast receiver access control.
ipv6 multicast boundary scope	Configures a multicast boundary on the interface for a specified scope.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
(config)# ipv6 multicast pim-passive-enable
```

Related Commands

Command	Description
ipv6 pim passive	Configures PIM passive mode on a specific interface.

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	The time range is from 1 through 65536 seconds. The default is 14 or 4 hours.
refresh	(Optional) Automatically refreshes the neighbor discovery cache e

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

By default, a neighbor discovery cache entry is expired and deleted if it remains in the STALE state for 14,400 seconds or 4 hours. The **ipv6 nd cache expire** command allows the expiry time to vary and to trigger auto refresh of an expired entry before the entry is deleted.

When the **refresh** keyword is used, a neighbor discovery cache entry is auto refreshed. The entry moves into the DELAY state and the neighbor unreachability detection process occurs, in which the entry transitions from the DELAY state to the PROBE state after 5 seconds. When the entry reaches the PROBE state, a neighbor solicitation is sent and then retransmitted as per the configuration.

Examples

The following example shows that the neighbor discovery cache entry is configured to expire in 7200 seconds or 2 hours:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/1/4
Device(config-if)# ipv6 nd cache expire 7200
```

Related Commands

Command	Description
ipv6 nd na glean	Configures neighbor discovery to glean an entry from an unsolicited neighbor advertisement.
ipv6 nd nud retry	Configures the number of times neighbor unreachability detection resends neighbor solicitations.
show ipv6 interface	Displays the usability status of interfaces that are configured for IPv6.

ipv6 nd 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*]

Syntax Description

size	Cache size.
log *rate*	(Optional) Adjustable logging rate, in seconds. The valid values are 0 and 1.

Command Default

Default logging rate for the device is one entry every second.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
(config)# ipv6 nd cache interface-limit 4
```

Related Commands

Command	Description
ipv6 nd cache interface-limit (interface)	Configures a neighbor discovery cache limit on a specified interface on the device.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
(config)# ipv6 nd host mode strict
(config-if)# interface ethernet0/0
(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:

```
(config)# ipv6 nd host mode strict
(config-if)# interface ethernet0/0
(config-if)# ipv6 address 2001::1/64
```

Related Commands

Command	Description
ipv6 unicast-routing	Enables the forwarding of IPv6 unicast datagrams.

ipv6 nd na glean

To configure the neighbor discovery to glean an entry from an unsolicited neighbor advertisement, use the **ipv6 nd na glean** command in the interface configuration mode. To disable this feature, use the **no** form of this command.

ipv6 nd na glean
no ipv6 nd na glean

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

IPv6 nodes may emit a multicast unsolicited neighbor advertisement packet following the successful completion of duplicate address detection (DAD). By default, other IPv6 nodes ignore these unsolicited neighbor advertisement packets. The **ipv6 nd na glean** command configures the router to create a neighbor advertisement entry on receipt of an unsolicited neighbor advertisement packet (assuming no such entry already exists and the neighbor advertisement has the link-layer address option). Use of this command allows a device to populate its neighbor advertisement cache with an entry for a neighbor before data traffic exchange with the neighbor.

Examples

The following example shows how to configure neighbor discovery to glean an entry from an unsolicited neighbor advertisement:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/1/4
Device(config-if)# ipv6 nd na glean
```

Related Commands

Command	Description
ipv6 nd cache expire	Configures the duration of time before an IPv6 neighbor discovery cache entry expires.
ipv6 nd nud retry	Configures the number of times neighbor unreachability detection resends neighbor solicitations.
show ipv6 interface	Displays the usability status of interfaces that are configured for IPv6.

ipv6 nd 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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
(config)# interface ethernet 0/0
(config-if)# ipv6 nd ns-interval 9000
```

Related Commands

Command	Description
ipv6 nd dad time	Configures the NS retransmit interval for DAD separately from the NS retransmit interval for address resolution.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 nd nud retry

To configure the number of times the neighbor unreachability detection process resends neighbor solicitations, use the **ipv6 nd nud retry** command in the interface configuration mode. To disable this feature, use the **no** form of this command.

ipv6 nd nud retry *base interval max-attempts* {*final-wait-time*}
no ipv6 nd nud retry *base interval max-attempts* {*final-wait-time*}

Syntax Description

base	The neighbor unreachability detection process base value.
interval	The time interval, in milliseconds, between retries. The range is from 1000 to 32000.
max-attempts	The maximum number of retry attempts, depending on the base The range is from 1 to 128.
final-wait-time	The waiting time, in milliseconds, on the last probe. The range is from 1000 to 32000.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

When a device runs neighbor unreachability detection to resolve the neighbor detection entry for a neighbor again, it sends three neighbor solicitation packets 1 second apart. In certain situations, for example, spanning-tree events, or high-traffic events, or end-host reloads), three neighbor solicitation packets that are sent at an interval of 1 second may not be sufficient. To help maintain the neighbor cache in such situations, use the **ipv6 nd nud retry** command to configure exponential timers for neighbor solicitation retransmits.

The maximum number of retry attempts is configured using the *max-attempts* argument. The retransmit interval is calculated with the following formula:

tm^n

here,

- t = Time interval
- m = Base (1, 2, or 3)
- n = Current neighbor solicitation number (where the first neighbor solicitation is 0).

Therefore, **ipv6 nd nud retry 3 1000 5** command retransmits at intervals of 1,3,9,27,81 seconds. If the final wait time is not configured, the entry remains for 243 seconds before it is deleted.

The **ipv6 nd nud retry** command affects only the retransmit rate for the neighbor unreachability detection process, and not for the initial resolution, which uses the default of three neighbor solicitation packets sent 1 second apart.

Examples

The following example shows how to configure a fixed interval of 1 second and three retransmits:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/1/4
Device(config-if)# ipv6 nd nud retry 1 1000 3
```

The following example shows how to configure a retransmit interval of 1, 2, 4, and 8:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/1/4
Device(config-if)# ipv6 nd nud retry 2 1000 4
```

The following example shows how to configure the retransmit intervals of 1, 3, 9, 27, 81:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/1/4
Device(config-if)# ipv6 nd nud retry 3 1000 5
```

Related Commands

Command	Description
ipv6 nd cache expire	Configures the duration of time before an IPv6 neighbor discovery (ND) cache entry expires.
ipv6 nd na glean	Configures neighbor discovery to glean an entry from an unsolicited neighbor advertisement.
show ipv6 interface	Displays the usability status of interfaces that are configured for IPv6.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
(config)# interface ethernet 0/0
(config-if)# ipv6 nd reachable-time 1700000
```

Related Commands

Command	Description
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
(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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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

```
(config)# ipv6 nd route-owner
```

Related Commands

Command	Description
ipv6 nd autoconfig default	Allows Neighbor Discovery to install a default route to the Neighbor Discovery-derived default router.
ipv6 nd autoconfig prefix	Uses Neighbor Discovery to install all valid on-link prefixes from RAs received on the interface.

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

ipv6-address	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.
interface-type	The specified interface type. For supported interface types, use the question mark (?) online help function.
interface-number	The specified interface number.
hardware-address	The local data-link address (a 48-bit address).

Command Default

Static entries are not configured in the IPv6 neighbor discovery cache.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
(config)# ipv6 neighbor 2001:0DB8::45A ethernet1 0002.7D1A.9472
```

Related Commands

Command	Description
arp (global)	Adds a permanent entry in the ARP cache.
clear ipv6 neighbors	Deletes all entries in the IPv6 neighbor discovery cache, except static entries.
no ipv6 enable	Disables IPv6 processing on an interface that has not been configured with an explicit IPv6 address.
no ipv6 unnumbered	Disables IPv6 on an unnumbered interface.
show ipv6 neighbors	Displays IPv6 neighbor discovery cache information.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
(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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
(config)# interface FastEthernet 1/0
(config-if)# no ipv6 pim
```

Related Commands

Command	Description
ipv6 multicast-routing	Enables multicast routing using PIM and MLD on all IPv6-enabled interfaces of the router and enables multicast forwarding.

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

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
list *access-list*	Defines the access list name.
route-map *map-name*	Defines the route map.

Command Default

All sources are accepted at the RP.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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 route:

```
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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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

Command	Description
ipv6 pim rp-address	Statically configures the address of a PIM RP for multicast groups.

ipv6 pim neighbor-filter list

To filter Protocol Independent Multicast (PIM) neighbor messages from specific IPv6 addresses, use the **ipv6 pim neighbor-filter** 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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
(config)# ipv6 pim neighbor-filter list nbr_filter_acl
(config)# ipv6 access-list nbr_filter_acl
(config-ipv6-acl)# deny ipv6 host FE80::A8BB:CCFF:FE03:7200 any
(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**]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
ipv6-address	The IPv6 address of a router to be a PIM RP. The *ipv6-address*argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
group-access-list	(Optional) Name of an access list that defines for which multicast groups the RP should be used. 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. 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. Note that the embedded RP group ranges need not include all the scopes (for example, 3 through 7).
bidir	(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. A single group-range list can be configured to operate either in bidirectional or sparse mode.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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-f]::/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:

```
(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:

```
(config)# ipv6 access-list acc-grp-1
(config-ipv6-acl)# permit ipv6 any ff04::/64
(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:

```
(config)# ipv6 pim rp-address 2001:0DB8:2::2 embd-ranges
(config)# ipv6 access-list embd-ranges
(config-ipv6-acl)# permit ipv6 any ff73:240:2:2:2::/96
(config-ipv6-acl)# permit ipv6 any ff74:240:2:2:2::/96
(config-ipv6-acl)# permit ipv6 any ff75:240:2:2:2::/96
(config-ipv6-acl)# permit ipv6 any ff76:240:2:2:2::/96
(config-ipv6-acl)# permit ipv6 any ff77:240:2:2:2::/96
(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.

```
(config)# ipv6 access-list bidir-grps
(config-ipv6-acl)# permit ipv6 any ff05::/16
(config-ipv6-acl)# permit ipv6 any ff06::/16
(config-ipv6-acl)# exit
(config)# ipv6 pim rp-address 200::1 bidir-grps bidir
```

Related Commands

Command	Description
debug ipv6 pim df-election	Displays debug messages for PIM bidirectional DF-election message processing.
ipv6 access-list	Defines an IPv6 access list and places the router in IPv6 access list configuration mode.
show ipv6 pim df	Displays the DF -election state of each interface for each RP.
show ipv6 pim df winner	Displays the DF-election winner on each interface for each RP.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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 fffX::/16. When the router is enabled, it parses groups in the embedded RP group ranges ff7X::/16 and fffX::/16, and extracts the RP to be used from the group address.

Examples

The following example disables embedded RP support in IPv6 PIM:

```
# 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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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.:

```
(config)# ipv6 access-list acc-grp-1
(config-ipv6-acl)# permit ipv6 any FF04::/64
(config-ipv6-acl)# exit
(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.

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

list-name	Name of the prefix list. • Cannot be the same name as an existing access list. • Cannot be the name "detail" or "summary" because they are keywords in the **show ipv6 prefix-list** command.
seq *seq-number*	(Optional) Sequence number of the prefix list entry being configured.
deny	Denies networks that matches the condition.
permit	Permits networks that matches the condition.
ipv6-prefix	The IPv6 network assigned to the specified prefix list. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
/*prefix-length*	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.
description *text*	A description of the prefix list that can be up to 80 characters in length.
ge *ge-value*	(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).
le *le-value*	(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).

Command Default

No prefix list is created.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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.

Note 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 any statement as its last match condition.

Examples

The following example denies all routes with a prefix of ::/0.

```
(config)# ipv6 prefix-list abc deny ::/0
```

The following example permits the prefix 2002::/16:

```
(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.

```
(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.

```
(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.

```
(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.

```
(config)# ipv6 prefix-list abc deny ::/0 ge 32
```

The following example denies all routes with a prefix of 2002::/128.

```
(config)# ipv6 prefix-list abc deny 2002::/128
```

The following example permits all routes with a prefix of ::/0.

```
(config)# ipv6 prefix-list abc permit ::/0
```

Related Commands

Command	Description
clear ipv6 prefix-list	Resets the hit count of the IPv6 prefix list entries.
distribute-list out	Suppresses networks from being advertised in updates.
ipv6 prefix-list sequence-number	Enables the generation of sequence numbers for entries in an IPv6 prefix list.
match ipv6 address	Distributes IPv6 routes that have a prefix permitted by a prefix list.
show ipv6 prefix-list	Displays information about an IPv6 prefix list or IPv6 prefix list entries.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
(config)# interface gigabitethernet 0/0/1
(config-if)# ipv6 source-guard attach-policy mysnoopingpolicy
```

Related Commands

Command	Description
ipv6 snooping policy	Configures an IPv6 snooping policy and enters IPv6 snooping configuration mode.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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

Command	Description
deny (IPv6)	Sets deny conditions for an IPv6 access list.

Command	Description
ipv6 icmp error-interval	Configures the interval for IPv6 ICMP error messages.

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

aggressive	Aggressive drop mode discards incorrectly formatted packets when the IPv6 SPD is in random drop state.
tos protocol o spf	OSPF mode allows OSPF packets to be handled with SPD priority.

Command Default

No IPv6 SPD mode is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
(config)# ipv6 spf mode aggressive
```

Related Commands

Command	Description
ipv6 spd queue max-threshold	Configures the maximum number of packets in the IPv6 SPD process input queue.
ipv6 spd queue min-threshold	Configures the minimum number of packets in the IPv6 SPD process input queue.
show ipv6 spd	Displays the IPv6 SPD configuration.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
(config)# ipv6 spd queue max-threshold 60000
```

Related Commands

Command	Description
ipv6 spd queue min-threshold	Configures the minimum number of packets in the IPv6 SPD process input queue.
show ipv6 spd	Displays the IPv6 SPD configuration.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
(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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
(config)# ipv6 unicast-routing
```

Related Commands

Command	Description
ipv6 address link-local	Configures an IPv6 link-local address for an interface and enables IPv6 processing on the interface.
ipv6 address eui-64	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.
ipv6 enable	Enables IPv6 processing on an interface that has not been configured with an explicit IPv6 address.
ipv6 unnumbered	Enables IPv6 processing on an interface without assigning an explicit IPv6 address to the interface.
show ipv6 route	Displays the current contents of the IPv6 routing 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)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

You must configure a key chain with keys to enable authentication.

Although you can identify multiple key chains, we recommend using one key chain per interface per routing protocol. Upon specifying the **key chain** command, you enter key chain configuration mode.

Examples

The following example shows how to specify key chain:

```
Device(config-keychain-key)# key-string chestnut
```

Related Commands

Command	Description
accept-lifetime	Sets the time period during which the authentication key on a key chain is received as valid.
key	Identifies an authentication key on a key chain.
key-string (authentication)	Specifies the authentication string for a key.
send-lifetime	Sets the time period during which an authentication key on a key chain is valid to be sent.
show key chain	Displays authentication key information.

key-string (authentication)

To specify the authentication string for a key, use the **key-string**(authentication) command in key chain key configuration mode. To remove the authentication string, use the **no** form of this command.

key-string key-string *text*
no key-string *text*

Syntax Description

text	Authentication string that must be sent and received in the packets using the routing protocol being authenticated. The string can contain from 1 to 80 uppercase and lowercase alphanumeric characters.

Command Default

No authentication string for a key exists.

Command Modes

Key chain key configuration (config-keychain-key)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Examples

The following example shows how to specify the authentication string for a key:

```
Device(config-keychain-key)# key-string key1
```

Related Commands

Command	Description
accept-lifetime	Sets the time period during which the authentication key on a key chain is received as valid.
key	Identifies an authentication key on a key chain.
key chain	Defines an authentication key-chain needed to enable authentication for routing protocols.
send-lifetime	Sets the time period during which an authentication key on a key chain is valid to be sent.
show key chain	Displays authentication key information.

key

To identify an authentication key on a key chain, use the **key** command in key-chain configuration mode. To remove the key from the key chain, use the **no** form of this command.

key *key-id*
no key *key-id*

Syntax Description

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 Default

No key exists on the key chain.

Command Modes

Key-chain configuration (config-keychain)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

It is useful to have multiple keys on a key chain so that the software can sequence through the keys as they become invalid after time, based on the **accept-lifetime** and **send-lifetime** key chain key command settings.

Each key has its own key identifier, which is stored locally. The combination of the key identifier and the interface associated with the message uniquely identifies the authentication algorithm and Message Digest 5 (MD5) authentication key in use. Only one authentication packet is sent, regardless of the number of valid keys. The software starts looking at the lowest key identifier number and uses the first valid key.

If the last key expires, authentication will continue and an error message will be generated. To disable authentication, you must manually delete the last valid key.

To remove all keys, remove the key chain by using the **no key chain** command.

Examples

The following example shows how to specify a key to identify authentication on a key-chain:

```
Device(config-keychain)# key 1
```

Related Commands

Command	Description
accept-lifetime	Sets the time period during which the authentication key on a key chain is received as valid.
key chain	Defines an authentication key chain needed to enable authentication for routing protocols.
key-string (authentication)	Specifies the authentication string for a key.
send-lifetime	Sets the time period during which an authentication key on a key chain is valid to be sent.

Command	Description
show key chain	Displays authentication key information.

show ip ports all

To display all the open ports on a device, use the **show ip ports all** in user EXEC or privileged EXEC mode.

show ip ports all

Syntax Description

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

This command provides a list of all open TCP/IP ports on the system including the ports opened using Cisco networking stack.

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 *:* 0/[IOS] Unknown
udp *:2228 10.0.0.0:0 318/[IOS]L2TRACE SERVER
```

The table below describes the significant fields shown in the display

Table 27: Field Descriptions of show ip ports all

Field	Description
Protocol	Transport protocol used.

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

Command	Description
show tcp brief all	Displays information about TCP connection endpoints.
show ip sockets	Displays IP sockets information.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
# show ipv6 access-list
IPv6 access list inbound
    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 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:

```
#  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 28: show ipv6 access-list Field Descriptions

Field	Description
ipv6 access list inbound	Name of the IPv6 access list, for example, inbound.

Field	Description
permit	Permits any packet that matches the specified protocol type.
tcp	Transmission Control Protocol. The higher-level (Layer 4) protocol type that the packet must match.
any	Equal to ::/0.
eq	An equal operand that compares the source or destination ports of TCP or UDP packets.
reflect	Indicates a reflexive IPv6 access list.
tcptraffic (8 matches)	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.
sequence 10	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).
host 2001:0DB8:1::1	The source IPv6 host address that the source address of the packet must match.
host 2001:0DB8:1::2	The destination IPv6 host address that the destination address of the packet must match.
11000	The ephemeral source port number for the outgoing connection.
timeout 300	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.
(time left 243)	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.
evaluate udptraffic	Indicates the IPv6 reflexive access list named udptraffic is nested in the IPv6 access list named outbound.

Related Commands

Command	Description
clear ipv6 access-list	Resets the IPv6 access list match counters.
hardware statistics	Enables the collection of hardware statistics.
show ip access-list	Displays the contents of all current IP access lists.
show ip prefix-list	Displays information about a prefix list or prefix list entries.
show ipv6 prefix-list	Displays information about an IPv6 prefix list or IPv6 prefix list entries.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
# show ipv6 destination-guard policy pol1
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:

```
# show ipv6 destination-guard policy pol1
Destination guard policy destination:
  enforcement always
        Target: Gi0/0/1
```

Related Commands

Command	Description
ipv6 destination-guard policy	Defines the destination guard policy.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
# 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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The **show ipv6 dhcp binding** command displays all automatic client bindings from the DHCP for IPv6 server binding table if the *ipv6-address* argument is not specified. When the *ipv6-address* argument is specified, only the binding for the specified client is displayed.

If the **vrf** *vrf-name*keyword and argument combination is specified, all bindings that belong to the specified VRF are displayed.

Note The **ipv6 dhcp server vrf enable** command must be enabled for the configured VRF to work. If the command is not configured, the output of the **show ipv6 dhcp binding** command will not display the configured VRF; it will only display the default VRF details.

Examples

The following sample output displays all automatic client bindings from the DHCP for IPv6 server binding table:

```
# show ipv6 dhcp binding

Client: FE80::A8BB:CCFF:FE00:300
  DUID: 00030001AABBCC000300
  Username : client_1
  Interface: Virtual-Access2.1
  IA PD: IA ID 0x000C0001, T1 75, T2 135
    Prefix: 2001:380:E00::/64
            preferred lifetime 150, valid lifetime 300
            expires at Dec 06 2007 12:57 PM (262 seconds)
Client: FE80::A8BB:CCFF:FE00:300 (Virtual-Access2.2)
  DUID: 00030001AABBCC000300
  IA PD: IA ID 0x000D0001, T1 75, T2 135
    Prefix: 2001:0DB8:E00:1::/64
```

```
            preferred lifetime 150, valid lifetime 300
            expires at Dec 06 2007 12:58 PM (288 seconds)
```

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

Table 29: show ipv6 dhcp binding Field Descriptions

Field	Description
Client	Address of a specified client.
DUID	DHCP unique identifier (DUID).
Virtual-Access2.1	First virtual client. When an IPv6 DHCP client requests two prefixes with the same DUID but a different identity association for prefix delegation (IAPD) on two different interfaces, these prefixes are considered to be for two different clients, and interface information is maintained for both.
Username : client_1	The username associated with the binding.
IA PD	Collection of prefixes assigned to a client.
IA ID	Identifier for this IAPD.
Prefix	Prefixes delegated to the indicated IAPD on the specified client.
preferred lifetime, valid lifetime	The preferred lifetime and valid lifetime settings, in seconds, for the specified client.
Expires at	Date and time at which the valid lifetime expires.
Virtual-Access2.2	Second virtual client. When an IPv6 DHCP client requests two prefixes with the same DUID but different IAIDs on two different interfaces, these prefixes are considered to be for two different clients, and interface information is maintained for both.

When the DHCPv6 pool on the Cisco IOS DHCPv6 server is configured to obtain prefixes for delegation from an authentication, authorization, and accounting (AAA) server, it sends the PPP username from the incoming PPP session to the AAA server for obtaining the prefixes. The PPP username 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":

```
# 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:

```
# 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: 2001:0DB8:1:1::/80
            preferred lifetime 300, valid lifetime 300
            expires at Aug 11 2008 06:23 AM (233 seconds)
```

Related Commands

Command	Description
ipv6 dhcp server vrf enable	Enables the DHCPv6 server VRF-aware feature.
clear ipv6 dhcp binding	Deletes automatic client bindings from the DHCP for IPv6 binding table.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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.:

```
# show ipv6 dhcp conflict
Pool 350, prefix 2001:0DB8:1005::/48
     2001:0DB8:1005::10
```

Related Commands

Command	Description
clear ipv6 dhcp conflict	Clears an address conflict from the DHCPv6 server database.

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*]

Syntax Description

agent-URL	(Optional) A flash, NVRAM, FTP, TFTP, or remote copy protocol (RCP) uniform resource locator.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
# 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
```

```
successful read times 0
failed read times 0
successful write times 2220
failed write times 614
```

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

Table 30: show ipv6 dhcp database Field Descriptions

Field	Description
Database agent	Specifies the database agent.
Write delay	The amount of time (in seconds) to wait before updating the database.
transfer timeout	Specifies how long (in seconds) the DHCP server should wait before canceling a database transfer. Transfers that exceed the timeout period are canceled.
Last written	The last date and time bindings were written to the file server.
Write timer expires...	The length of time, in seconds, before the write timer expires.
Last read	The last date and time bindings were read from the file server.
Successful/failed read times	The number of successful or failed read times.
Successful/failed write times	The number of successful or failed write times.

Related Commands

Command	Description
ipv6 dhcp database	Specifies DHCP for IPv6 binding database agent parameters.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
# 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 31: show ipv6 dhcp guard Field Descriptions

Field	Description
Device Role	The role of the device. The role is either client, server or relay.
Target	The name of the target. The target is either an interface or a VLAN.

Related Commands

Command	Description
ipv6 dhcp guard policy	Defines the DHCPv6 guard policy name.

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.

show ipv6 dhcp interface [*type number*]

Syntax Description

type number	(Optional) Interface type and number. For more information, use the question mark (**?**) online help function.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
# 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
```

```
    Prefix name is cli-p1
    Rapid-Commit is enabled
```

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

Table 32: show ipv6 dhcp interface Field Descriptions

Field	Description
Ethernet2/1 is in server/client mode	Displays whether the specified interface is in server or client mode.
Preference value:	The advertised (or default of 0) preference value for the indicated server.
Prefix name is cli-p1	Displays the IPv6 general prefix pool name, in which prefixes successfully acquired on this interface are stored.
Using pool: svr-p1	The name of the pool that is being used by the interface.
State is OPEN	State of the DHCP for IPv6 client on this interface. "Open" indicates that configuration information has been received.
List of known servers	Lists the servers on the interface.
Address, DUID	Address and DHCP unique identifier (DUID) of a server heard on the specified interface.
Rapid commit is disabled	Displays whether the **rapid-commit** keyword has been enabled on the interface.

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:

```
(config-if)# ipv6 dhcp relay destination FE80::250:A2FF:FEBF:A056 FastEthernet0/1
# 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

Command	Description
ipv6 dhcp client pd	Enables the DHCP for IPv6 client process and enables requests for prefix delegation through a specified interface.
ipv6 dhcp relay destination	Specifies a destination address to which client messages are forwarded and enables DHCP for IPv6 relay service on the interface.
ipv6 dhcp server	Enables DHCP for IPv6 service on an interface.

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

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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: 000300010023BED94D31
  IAID: 3201912114
  lifetime: 600
```

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

Table 33: show ipv6 dhcp relay binding Field Descriptions

Field	Description
Prefix	IPv6 prefix for DHCP.

Field	Description
DUID	DHCP Unique Identifier (DUID) for the IPv6 relay binding.
IAID	Identity Association Identification (IAID) for DHCP.
lifetime	Lifetime of the prefix, in seconds.

Related Commands

Command	Description
clear ipv6 dhcp relay binding	Clears a specific IPv6 address or IPv6 prefix of a DHCP for IPv6 relay binding.
debug ipv6 dhcp relay	Enables debugging for IPv6 DHCP relay agent.
debug ipv6 dhcp relay bulk-lease	Enables bulk lease query debugging for IPv6 DHCP relay agent.

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

errmsg	(Optional) Displays error messages being logged.
sia	(Optional) Displays Stuck In Active (SIA) messages.
event-num-start	(Optional) Starting number of the event range. The range is from 1 to 4294967295.
event-num-end	(Optional) Ending number of the event range. The range is from 1 to 4294967295.
type	(Optional) Displays event types being logged.

Command Default

If no event range is specified, information for all IPv6 EIGRP events is displayed.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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.

```
# 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
```

```
16   00:56:41.687 Rcv query dest/nh: 2555:5555::/32 FE80::ABCD:4:EF00:2
17   00:56:41.687 State change: Local origin Successor Origin
18   00:56:41.687 Metric set: 2555:5555::/32 4294967295
19   00:56:41.687 Active net/peers: 2555:5555::/32 65536
20   00:56:41.687 FC not sat Dmin/met: 4294967295 2588160
21   00:56:41.687 Find FS: 2555:5555::/32 2588160
22   00:56:41.687 Rcv query met/succ met: 4294967295 4294967295
23   00:56:41.687 Rcv query dest/nh: 2555:5555::/32 FE80::ABCD:4:EF00:1
24   00:56:41.659 Change queue emptied, entries: 1
25   00:56:41.659 Metric set: 2555:5555::/32 2588160
```

Related Commands

Command	Description
clear ipv6 eigrp	Deletes entries from EIGRP for IPv6 routing tables.
debug ipv6 eigrp	Displays information about EIGRP for IPv6 protocol.
ipv6 eigrp	Enables EIGRP for IPv6 on a specified interface.

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**]

Syntax Description

as-number	(Optional) Autonomous system number.
type	(Optional) Interface type. For more information, use the question mark (?) online help function.
number	(Optional) Interface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
detail	(Optional) Displays detailed interface information.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
# show ipv6 eigrp 1 interfaces

IPv6-EIGRP interfaces for process 1
                    Xmit Queue    Mean    Pacing Time    Multicast     Pending
Interface    Peers  Un/Reliable   SRTT    Un/Reliable    Flow Timer    Routes
Et0/0         0         0/0          0        0/10            0          0
```

The following is sample output from the **show ipv6 eigrp interfaces detail** command:

```
# show ipv6 eigrp interfaces detail

IPv6-EIGRP interfaces for process 1
                    Xmit Queue    Mean    Pacing Time    Multicast    Pending
Interface    Peers  Un/Reliable   SRTT    Un/Reliable    Flow Timer    Routes
Et0/0          0        0/0          0        0/10            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:

```
Device# show ipv6 eigrp interfaces detail tunnel 0

EIGRP-IPv6 Interfaces for AS(1)
                       Xmit Queue   PeerQ        Mean   Pacing Time   Multicast   Pending

Interface        Peers  Un/Reliable  Un/Reliable  SRTT   Un/Reliable   Flow Timer   Routes
Tu0/0              2        0/0       0/0          29       0/0         136           0
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 34: show ipv6 eigrp interfaces Field Descriptions

Field	Description
Interface	Interface over which EIGRP is configured.
Peers	Number of directly connected EIGRP neighbors.
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 in which the device will send multicast EIGRP packets.
Pending Routes	Number of routes in the transmit queue waiting to be sent.
Hello interval is 5 sec	Length (in seconds) of the hello interval.

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

as-number	(Optional) Autonomous system number.
ipv6-address	(Optional) IPv6 address.
active	(Optional) Displays only active entries in the EIGRP topology table.
all-links	(Optional) Displays all entries in the EIGRP topology table (including nonfeasible-successor sources).
pending	(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.
summary	(Optional) Displays a summary of the EIGRP topology table.
zero-successors	(Optional) Displays the available routes that have zero successors.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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.

```
# 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.

```
# 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
```

Related Commands

Command	Description
show eigrp address-family topology	Displays entries in the EIGRP topology 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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
# 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 35: show ipv6 eigrp traffic Field Descriptions

Field	Description
process 9	Autonomous system number specified in the **ipv6 router eigrp**command.
Hellos sent/received	Number of hello packets sent and received.
Updates sent/received	Number of update packets sent and received.
Queries sent/received	Number of query packets sent and received.
Replies sent/received	Number of reply packets sent and received.
Acks sent/received	Number of acknowledgment packets sent and received.

Related Commands

Command	Description
ipv6 router eigrp	Configures the EIGRP for IPv6 routing process.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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.

```
# 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 36: show ipv6 general-prefix Field Descriptions

Field	Description
IPv6 Prefix	User-defined name of the IPv6 general prefix.
Acquired via	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.
2002:B0B:B0B::/48	The prefix value for this general prefix.
Loopback42 (Address command)	List of interfaces where this general prefix is used.

Related Commands

Command	Description
ipv6 general-prefix	Defines a general prefix for an IPv6 address manually.

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.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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.

```
(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
```

```
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 unreachables 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 37: show ipv6 interface Field Descriptions

Field	Description
Ethernet0/0 is up, line protocol is up	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 "up." For an interface to be usable, both the interface hardware and line protocol must be up.
line protocol is up, down (down is not shown in sample output)	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.
IPv6 is enabled, stalled, disabled (stalled and disabled are not shown in sample output)	Indicates that IPv6 is enabled, stalled, or disabled on the interface. If IPv6 is enabled, the interface is marked "enabled." 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 "stalled." If IPv6 is not enabled, the interface is marked "disabled."
link-local address	Displays the link-local address assigned to the interface.
Global unicast address(es):	Displays the global unicast addresses assigned to the interface.
Joined group address(es):	Indicates the multicast groups to which this interface belongs.
MTU	Maximum transmission unit of the interface.
ICMP error messages	Specifies the minimum interval (in milliseconds) between error messages sent on this interface.
ICMP redirects	The state of Internet Control Message Protocol (ICMP) IPv6 redirect messages on the interface (the sending of the messages is enabled or disabled).

Field	Description
ND DAD	The state of duplicate address detection on the interface (enabled or disabled).
number of DAD attempts:	Number of consecutive neighbor solicitation messages that are sent on the interface while duplicate address detection is performed.
ND reachable time	Displays the neighbor discovery reachable time (in milliseconds) assigned to this interface.
ND advertised reachable time	Displays the neighbor discovery reachable time (in milliseconds) advertised on this interface.
ND advertised retransmit interval	Displays the neighbor discovery retransmit interval (in milliseconds) advertised on this interface.
ND router advertisements	Specifies the interval (in seconds) for neighbor discovery router advertisements (RAs) sent on this interface and the amount of time before the advertisements expire. As of Cisco IOS Release 12.4(2)T, this field displays the default router preference (DRP) value sent by this device on this interface.
ND advertised default router preference is Medium	The DRP for the device on a specific interface.

The **show ipv6 interface** command displays information about attributes that may be associated with an IPv6 address assigned to the interface.

Attribute	Description
ANY	Anycast. The address is an anycast address, as specified when configured using the **ipv6 address** command.
CAL	Calendar. The address is timed and has valid and preferred lifetimes.
DEP	Deprecated. The timed address is deprecated.
DUP	Duplicate. The address is a duplicate, as determined by duplicate address detection (DAD). To re-attampt DAD, the user must use the **shutdown** or **no shutdown** command on the interface.
EUI	EUI-64 based. The address was generated using EUI-64.
OFF	Offlink. The address is offlink.

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:

```
# 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:

```
# 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:

```
# 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:

```
# 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 38: show ipv6 interface Command with HSRP Configured Field Descriptions

Field	Description
IPv6 is enabled, link-local address is FE80:2::2 [UNA]	The interface IPv6 link-local address is marked UNA because it is no longer advertised.
FE80::205:73FF:FEA0:1 [UNA/TEN]	The virtual link-local address list with the UNA and TEN attributes set.
FF02::66	HSRP IPv6 multicast address.
FE80::205:73FF:FEA0:1 [OPT]	HSRP becomes active, and the HSRP virtual address marked OPT.
FF02::1:FFA0:1	HSRP solicited node multicast address.

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:

```
(config-if)# ipv6 nd ra-interval 100 60
```

Subsequent use of the **show ipv6 interface** then displays the interval as follows:

```
(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:

```
(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 39: show ipv6 interface Command with Minimum RA Interval Information Configuration Field Descriptions

Field	Description
ND router advertisements are sent every 60 to 100 seconds	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.
ND router advertisements are sent every 60 to 100 milliseconds	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.

Related Commands

Command	Description
ipv6 nd prefix	Configures which IPv6 prefixes are included in IPv6 router advertisements.
ipv6 nd ra interval	Configures the interval between IPv6 RA transmissions on an interface.
show ip interface	Displays the usability status of interfaces configured for IP.

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**}]

show ipv6 mfib [**vrf** *vrf-name*] [{**all** | **linkscope** | **verbose** | **interface** | **status** | **summary**}]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
all	(Optional) Displays all forwarding entries and interfaces in the IPv6 MFIB.
linkscope	(Optional) Displays the link-local groups.
verbose	(Optional) Provides additional information, such as the MAC encapsulation header and platform-specific information.
ipv6-prefix	(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.
/ *prefix-length*	(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.
group-address-name	(Optional) IPv6 address or name of the multicast group.
source-address-name	(Optional) IPv6 address or name of the multicast group.
interface	(Optional) Interface settings and status.
status	(Optional) General settings and status.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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 40: MFIB Entries and Interface Flags

Flag	Description
F	Forward--Data is forwarded out of this interface.
A	Accept--Data received on this interface is accepted for forwarding.
IC	Internal copy--Deliver to the router a copy of the packets received or forwarded on this interface.
NS	Negate signal--Reverse the default entry signaling behavior for packets received on this interface.
DP	Do not preserve--When signaling the reception of a packet on this interface, do not preserve a copy of it (discard it instead).
SP	Signal present--The reception of a packet on this interface was just signaled.
S	Signal--By default, signal the reception of packets matching this entry.
C	Perform directly connected check for packets matching this entry. Signal the reception if packets were originated by a directly connected source.

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:

```
# 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
   Tunnel0 Flags: NS
(*,FF00::/15) Flags: D
   Forwarding: 0/0/0/0, Other: 0/0/0
(*,FF05::1) Flags: C
   Forwarding: 2/0/100/0, Other: 0/0/0
   Tunnel0 Flags: A NS
   Ethernet1/1 Flags: F NS
     Pkts: 0/2
(2001::1:1:200,FF05::1) Flags:
   Forwarding: 5/0/100/0, Other: 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
```

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

Table 41: show ipv6 mfib Field Descriptions

Field	Description
Entry Flags	Information about the entry.
Forwarding Counts	Statistics on the packets that are received from and forwarded to at least one interface.
Pkt Count/	Total number of packets received and forwarded since the creation of the multicast forwarding state to which this counter applies.
Pkts per second/	Number of packets received and forwarded per second.
Avg Pkt Size/	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.
Kbits per second	Bytes per second divided by packets per second divided by 1000.
Other counts:	Statistics on the received packets. These counters include statistics about the packets received and forwarded and packets received but not forwarded.
Interface Flags:	Information about the interface.
Interface Counts:	Interface statistics.

The following example shows forwarding entries and interfaces in the MFIB, with a group address of FF03:1::1 specified:

```
# 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/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
*,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
.
```

```
.
.
GigabitEthernet5/0.16 Flags:F NS
Pkts:71628/24
```

The following example shows forwarding entries and interfaces in the MFIB, with a group address of FF03:1::1 and a source address of 5002:1::2 specified:

```
# show ipv6 mfib FF03:1::1 5002:1::2

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
(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
.
.
.
   GigabitEthernet5/0.16 Flags:F NS
     Pkts:71628/24
```

The following example shows forwarding entries and interfaces in the MFIB, with a group address of FF03:1::1 and a default prefix of 128:

```
# show ipv6 mfib FF03:1::1/128
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
(*,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
.
.
.
   GigabitEthernet5/0.16 Flags:F NS
     Pkts:0/0
```

The following example shows forwarding entries and interfaces in the MFIB, with a group address of FFE0 and a prefix of 15:

```
# 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.

```
# 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,
                MCG - 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 Forwd:   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: 33330001000100D0FFFE180086DD
```

The table below describes the fields shown in the display.

Table 42: show ipv6 mfib verbose Field Descriptions

Field	Description
Platform flags	Information about the platform.
Platform per slot HW-Forwarding Counts	Total number of packets per bytes forwarded.

Related Commands

Command	Description
show ipv6 mfib active	Displays the rate at which active sources are sending to multicast groups.
show ipv6 mfib count	Displays summary traffic statistics from the MFIB about the group and source.
show ipv6 mfib interface	Displays information about IPv6 multicast-enabled interfaces and their forwarding status.

Command	Description
show ipv6 mfib status	Displays the general MFIB configuration and operational status.
show ipv6 mfib summary	Displays summary information about the number of IPv6 MFIB entries (including link-local groups) and interfaces.

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-namegroup-address*}] [*interface-type interface-number*] [{**detail** | **explicit**}]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
link-local	(Optional) Displays the link-local groups.
group-name | *group-address*	(Optional) IPv6 address or name of the multicast group.
interface-type interface-number	(Optional) Interface type and number.
detail	(Optional) Displays detailed information about individual sources.
explicit	(Optional) Displays information about the hosts being explicitly tracked on each interface for each group.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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.

```
# 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:

```
# show ipv6 mld groups detail
Interface:      Ethernet2/1/1
Group:          FF33::1:1:1
Uptime:         00:00:11
Router mode:    INCLUDE
Host mode:      INCLUDE
Last reporter:  FE80::250:54FF:FE60:3B14
Group source list:
Source Address                          Uptime    Expires   Fwd  Flags
2004:4::6                               00:00:11  00:04:08  Yes  Remote Ac 4
```

The following is sample output from the **show ipv6 mld groups** command using the **explicit** keyword:

```
# show ipv6 mld groups explicit
Ethernet1/0, FF05::1
    Up:00:43:11 EXCLUDE(0/1) Exp:00:03:17
    Host Address                            Uptime   Expires
    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
    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 moe)
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 43: show ipv6 mld groups Field Descriptions

Field	Description
Group Address	Address of the multicast group.
Interface	Interface through which the group is reachable.
Uptime	How long (in hours, minutes, and seconds) this multicast group has been known.
Expires	How long (in hours, minutes, and seconds) until the entry is removed from the MLD groups table. The expiration timer shows "never" if the router itself has joined the group, and the expiration timer shows "not used" when the router mode of the group is INCLUDE. In this situation, the expiration timers on the source entries are used.
Last reporter:	Last host to report being a member of the multicast group.

Field	Description
Flags Ac 4	Flags counted toward the MLD state limits configured.

Related Commands

Command	Description
ipv6 mld query-interval	Configures the frequency at which the Cisco IOS software sends MLD host-query messages.

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

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
type number	(Optional) Interface type and number.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
# 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 44: show ipv6 mld interface Field Descriptions

Field	Description
Global State Limit: 2 active out of 2 max	Two globally configured MLD states are active.

Field	Description
Ethernet2/1/1 is up, line protocol is up	Interface type, number, and status.
Internet address is...	Internet address of the interface and subnet mask being applied to the interface.
MLD is enabled in interface	Indicates whether Multicast Listener Discovery (MLD) has been enabled on the interface with the **ipv6 multicast-routing** command.
Current MLD version is 2	The current MLD version.
MLD query interval is 125 seconds	Interval (in seconds) at which the Cisco IOS software sends MLD query messages, as specified with the **ipv6 mld query-interval** command.
MLD querier timeout is 255 seconds	The length of time (in seconds) before the router takes over as the querier for the interface, as specified with the **ipv6 mld query-timeout** command.
MLD max query response time is 10 seconds	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 **ipv6 mld query-max-response-time** command.
Last member query response interval is 1 seconds	Used to calculate the maximum response code inserted in group and source-specific query. Also used to tune the "leave latency" of the link. A lower value results in reduced time to detect the last member leaving the group.
Interface State Limit : 2 active out of 3 max	Two out of three configured interface states are active.
State Limit permit access list: change	Activity for the state permit access list.
MLD activity: 83 joins, 63 leaves	Number of groups joins and leaves that have been received.
MLD querying router is FE80::260:3EFF:FE86:5649 (this system)	IPv6 address of the querying router.

Related Commands

Command	Description
ipv6 mld join-group	Configures MLD reporting for a specified group and source.
ipv6 mld query-interval	Configures the frequency at which the Cisco IOS software sends MLD host-query messages.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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.

```
# 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.

```
# 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

Command	Description
ipv6 mld snooping	Enables and configures MLD snooping on the switch or on a VLAN.
sdm prefer	Configures an SDM template to optimize system resources based on how the switch is being used.

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

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
source-address	(Optional) Source address associated with an MLD membership for a group identified by the access list.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
# show ipv6 mld ssm-map
SSM Mapping  : Enabled
DNS Lookup   : Enabled
```

The following examples show SSM mapping for the source address 2001:0DB8::1:

```
# 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 45: show ipv6 mld ssm-map Field Descriptions

Field	Description
SSM Mapping	The SSM mapping feature is enabled.

Field	Description
DNS Lookup	The DNS lookup feature is automatically enabled when the SSM mapping feature is enabled.
Group address	Group address identified by a specific access list.
Group mode ssm : TRUE	The identified group is functioning in SSM mode.
Database : STATIC	The router is configured to determine source addresses by checking static SSM mapping configurations.
Database : DNS	The router is configured to determine source addresses using DNS-based SSM mapping.
Source list	Source address associated with a group identified by the access list.

Related Commands

Command	Description
debug ipv6 mld ssm-map	Displays debug messages for SSM mapping.
ipv6 mld ssm-map enable	Enables the SSM mapping feature for groups in the configured SSM range
ipv6 mld ssm-map query dns	Enables DNS-based SSM mapping.
ipv6 mld ssm-map static	Configures static SSM mappings.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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.

```
# 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 46: show ipv6 mld traffic Field Descriptions

Field	Description
Elapsed time since counters cleared	Indicates the amount of time (in hours, minutes, and seconds) since the counters cleared.
Valid MLD packets	Number of valid MLD packets received and sent.
Queries	Number of valid queries received and sent.

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*}]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
filter	(Optional) Displays information about MRIB flags that each client owns and that each client is interested in.
name	(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).
client-name **:** *client-id*	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.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
# 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 47: show ipv6 mrib client Field Descriptions

Field	Description
igmp:145 (connection id 0) pim:146 (connection id 1) mfib ipv6:3 (connection id 2) mfib ipv6 rp agent:16 (connection id 3)	Client ID (client name:process ID)

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-addresssource-name* | *****}] [*groupname-or-address* [*prefix-length*]]}]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
link-local	(Optional) Displays the link-local groups.
summary	(Optional) Displays the number of MRIB entries (including link-local groups) and interfaces present in the MRIB table.
source address-or-name	(Optional) IPv6 address or name of the source.
*****	(Optional) Displays all MRIB route information.
groupname or-address	(Optional) IPv6 address or name of the multicast group.
prefix-length	(Optional) IPv6 prefix length.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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 48: Description of Interface Flags

Flag	Description
F	Forward--Data is forwarded out of this interface
A	Accept--Data received on this interface is accepted for forwarding
IC	Internal copy
NS	Negate signal

Flag	Description
DP	Do not preserve
SP	Signal present
II	Internal interest
ID	Internal uninterest
LI	Local interest
LD	Local uninterest
C	Perform directly connected check

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:

```
# 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 49: show ipv6 mrib route Field Descriptions

Field	Description
No. of (*, G) routes	Number of shared tree routes in the MRIB.
No. of (S, G) routes	Number of source tree routes in the MRIB.
No. of Route x Interfaces (RxI)	Sum of all the interfaces on each MRIB route entry.

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-addresssource-name*}]}]}] [**summary**] [**count**]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
link-local	(Optional) Displays the link-local groups.
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.
summary	(Optional) Displays a one-line, abbreviated summary of each entry in the IPv6 multicast routing table.
count	(Optional) Displays statistics from the Multicast Forwarding Information Base (MFIB) about the group and source, including number of packets, packets per second, average packet size, and bytes per second.

Command Default

The **show ipv6 mroute** command displays all groups and sources.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
# 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:Tunnel5
  RPF nbr:6:6:6::6
  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:

```
# 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, OIF count:1, flags:S
(2001:0DB8:999::99, FF07::1), 00:02:17/00:01:12, OIF count:1, flags:SFT
```

The following is sample output from the **show ipv6 mroute** command with the **count** keyword:

```
# 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
   LC Forwarding:0/0/0/0, Other:0/0/0
  Source:2001:0DB8:999::99,
   RP Forwarding:0/0/0/0, Other:0/0/0
   LC Forwarding:0/0/0/0, Other:0/0/0
   HW Forwd:  20000/0/92/0, Other:0/0/0
  Tot. shown:Source count:1, pkt count:20000
```

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

Table 50: show ipv6 mroute Field Descriptions

Field	Description
Flags:	Provides information about the entry. • S--sparse. Entry is operating in sparse mode. • 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. • C--connected. A member of the multicast group is present on the directly connected interface. • L--local. The router itself is a member of the multicast group. • 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). • P--pruned. Route has been pruned. The Cisco IOS software keeps this information so that a downstream member can join the source. • 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. • F--register flag. Indicates that the software is registering for a multicast source. • T--SPT-bit set. Indicates that packets have been received on the shortest path source tree. • J--join SPT. For (*, 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 (*, G) entries and is never cleared. The router immediately switches to the shortest path source tree when traffic from a new source is received
Timers: Uptime/Expires	"Uptime" indicates per interface how long (in hours, minutes, and seconds) the entry has been in the IPv6 multicast routing table. "Expires" indicates per interface how long (in hours, minutes, and seconds) until the entry will be removed from the IPv6 multicast routing table.
Interface state:	Indicates the state of the incoming or outgoing interface. • Interface. Indicates the type and number of the interface listed in the incoming or outgoing interface list. • Next-Hop. "Next-Hop" specifies the IP address of the downstream neighbor. • State/Mode. "State" indicates that packets will either be forwarded, pruned, or null on the interface depending on whether there are restrictions due to access lists. "Mode" indicates that the interface is operating in sparse mode.

Field	Description
(*, FF07::1) and (2001:0DB8:999::99)	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.
RP	Address of the RP router.
flags:	Information set by the MRIB clients on this MRIB entry.
Incoming interface:	Expected interface for a multicast packet from the source. If the packet is not received on this interface, it is discarded.
RPF nbr	IP address of the upstream router to the RP or source.
Outgoing interface list:	Interfaces through which packets will be forwarded. For (S,G) entries, this list will not include the interfaces inherited from the (*,G) entry.

Related Commands

Command	Description
ipv6 multicast-routing	Enables multicast routing using PIM and MLD on all IPv6-enabled interfaces of the router and enables multicast forwarding.
show ipv6 mfib	Displays the forwarding entries and interfaces in the IPv6 MFIB.

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*]

Syntax Description

vrf	(Optional) Displays an IPv6 Virtual Private Network (VPN) routing/forwarding instance (VRF).
vrfname	(Optional) Name of the IPv6 VRF.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
# 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:

```
# 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 51: show ipv6 mtu Field Descriptions

Field	Description
MTU	MTU, which was contained in the Internet Control Message Protocol (ICMP) packet-too-big message, used for the path to the destination address.
Since	Age of the entry since the ICMP packet-too-big message was received.
Destination Address	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.

Related Commands

Command	Description
ipv6 mtu	Sets the MTU size of IPv6 packets sent on an interface.

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

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
interface- type	(Optional) Specifies the Interface type.
interface- number	(Optional) Specifies the Interface number.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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

```
# 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 52: show ipv6 nd destination Field Descriptions

Field	Description
Code: R - Redirect	Destinations learned through redirect.
2001::1 [8]	The value displayed in brackets is the time, in seconds, since the destination cache entry was last used.

Related Commands

Command	Description
ipv6 nd host mode strict	Enables the conformant, or strict, IPv6 host mode.

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

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
interface -type	(Optional) Specifies the Interface type.
interface -number	(Optional) Specifies the Interface number.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
# 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
2001:1:2::/64  [2591994/604794]
router FE80::A8BB:CCFF:FE00:5A00/Ethernet0/0
```

Related Commands

Command	Description
ipv6 nd host mode strict	Enables the conformant, or strict, IPv6 host mode.

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-numberipv6-addressipv6-hostname* | **statistics**}]

Syntax Description

interface-type	(Optional) Specifies the type of the interface from which IPv6 neighbor information is to be displayed.
interface-number	(Optional) Specifies the number of the interface from which IPv6 neighbor information is to be displayed.
ipv6-address	(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.
ipv6-hostname	(Optional) Specifies the IPv6 hostname of the remote networking device.
statistics	(Optional) Displays ND cache statistics.

Command Default

All IPv6 ND cache entries are listed.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
# show ipv6 neighbors ethernet 2
IPv6 Address                              Age Link-layer Addr State Interface
2000:0:0:4::2                               0 0003.a0d6.141e  REACH Ethernet2
FE80::203:A0FF:FED6:141E                    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:

```
# show ipv6 neighbors 2000:0:0:4::2
IPv6 Address                              Age Link-layer Addr State Interface
2000:0:0:4::2                               0 0003.a0d6.141e  REACH Ethernet2
```

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

Table 53: show ipv6 neighbors Field Descriptions

Field	Description
IPv6 Address	IPv6 address of neighbor or interface.
Age	Time (in minutes) since the address was confirmed to be reachable. A hyphen (-) indicates a static entry.
Link-layer Addr	MAC address. If the address is unknown, a hyphen (-) is displayed.
State	The state of the neighbor cache entry. Following are the states for dynamic entries in the IPv6 neighbor discovery cache: • 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. • 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. • 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. • 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. • PROBE--A reachability confirmation is actively sought by resending neighbor solicitation messages every RetransTimer milliseconds until a reachability confirmation is received. • ????--Unknown state. 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.
Interface	Interface from which the address was reachable.

The following is sample output from the **show ipv6 neighbors** command with the **statistics** keyword:

```
# 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 54: show ipv6 neighbors statistics Field Descriptions

Field	Description
Entries	Total number of ND neighbor entries in the ND cache.
High-Water	Maximum amount (so far) of ND neighbor entries in ND cache.
Gleaned	Number of ND neighbor entries gleaned (that is, learned from a neighbor NA or other ND packet).
Scavenged	Number of stale ND neighbor entries that have timed out and been removed from the cache.
Entry States	Number of ND neighbor entries in each state.
Resolutions (INCMP)	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: • Requested--Total number of resolutions requested. • Timeouts--Number of timeouts during resolutions. • Resolved--Number of successful resolutions. • Failed--Number of unsuccessful resolutions. • In-progress--Number of resolutions in progress. • High-water--Maximum number (so far) of resolutions in progress. • Throttled--Number of times resolution request was ignored due to maximum number of resolutions in progress limit. • Data discards--Number of data packets discarded that are awaiting neighbor resolution.

Field	Description
Resolutions (PROBE)	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.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

show ipv6 ospf Output Example

The following is sample output from the **show ipv6 ospf** command:

```
# show ipv6 ospf
Routing Process "ospfv3 1" with ID 10.10.10.1
 SPF schedule delay 5 secs, Hold time between two SPFs 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 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 55: show ipv6 ospf Field Descriptions

Field	Description
Routing process "ospfv3 1" with ID 10.10.10.1	Process ID and OSPF device ID.
LSA group pacing timer	Configured LSA group pacing timer (in seconds).
Interface flood pacing timer	Configured LSA flood pacing timer (in milliseconds).
Retransmission pacing timer	Configured LSA retransmission pacing timer (in milliseconds).
Number of areas	Number of areas in device, area addresses, and so on.

show ipv6 ospf With Area Encryption Example

The following sample output shows the **show ipv6 ospf** command with area encryption information:

```
# 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 SPFs 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 56: show ipv6 ospf with Area Encryption Information Field Descriptions

Field	Description
Area 1	Subsequent fields describe area 1.

Field	Description
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:

```
# 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 57: show ipv6 ospf with SPF and LSA Throttling Timer Field Descriptions

Field	Description
Initial SPF schedule delay	Delay time of SPF calculations.
Minimum hold time between two consecutive SPFs	Minimum hold time between consecutive SPF calculations.
Maximum wait time between two consecutive SPFs 10000 msecs	Maximum hold time between consecutive SPF calculations.
Minimum LSA interval 5 secs	Minimum time interval (in seconds) between link-state advertisements.
Minimum LSA arrival 1000 msecs	Maximum arrival time (in milliseconds) of link-state advertisements.

The following example shows information about LSAs that are currently being rate limited:

```
# show ipv6 ospf rate-limit
List of LSAs that are in rate limit Queue
    LSAID: 0.0.0.0 Type: 0x2001 Adv Rtr: 10.55.55.55 Due in: 00:00:00.500
    LSAID: 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 58: show ipv6 ospf rate-limit Field Descriptions

Field	Description
LSAID	Link-state ID of the LSA.
Type	Description of the LSA.

Field	Description
Adv Rtr	ID of the advertising device.
Due in:	Remaining time until the generation of the next event.

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

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.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Examples

The following is sample output from the **show ipv6 ospf border-routers** command:

```
# 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 59: show ipv6 ospf border-routers Field Descriptions

Field	Description
i - Intra-area route, I - Inter-area route	The type of this route.
172.16.4.4, 172.16.3.3	Router ID of the destination router.
[2], [1]	Metric used to reach the destination router.
FE80::205:5FFF:FED3:5808, FE80::205:5FFF:FED3:5406, FE80::205:5FFF:FED3:5808	Link-local routers.
FastEthernet0/0, POS4/0	The interface on which the IPv6 OSPF protocol is configured.
ABR	Area border router.

Field	Description
ASBR	Autonomous system boundary router.
Area 0, Area 1	The area ID of the area from which this route is learned.
SPF 13, SPF 8, SPF 3	The internal number of the shortest path first (SPF) calculation that installs this route.

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

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.
generic	(Optional) Generic information regarding OSPF for IPv6 events.
interface	(Optional) Interface state change events, including old and new states.
lsa	(Optional) LSA arrival and LSA generation events.
neighbor	(Optional) Neighbor state change events, including old and new states.
reverse	(Optional) Keyword to allow the display of events in reverse-from the latest to the oldest or from oldest to the latest.
rib	(Optional) Routing Information Base (RIB) update, delete, and redistribution events.
spf	(Optional) Scheduling and SPF run events.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
# 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
```

```
9 *Sep 29 11:59:18.367: Rcv Changed Type-0x2001 LSA, LSID 10.0.0.0, Adv-Rtr 1.1.1.1, Seq#
80007699, Age 2
10 *Sep 29 11:59:18.367: Schedule SPF, Area 0, Change in LSID 10.0.0.0, LSA type R
11 *Sep 29 11:59:18.867: Starting SPF
12 *Sep 29 11:59:18.867: Starting Intra-Area SPF in Area 0
16 *Sep 29 11:59:18.867: Starting Inter-Area SPF in area 0
17 *Sep 29 11:59:18.867: Starting External processing
18 *Sep 29 11:59:18.867: Starting External processing in area 0
19 *Sep 29 11:59:18.867: Starting External processing in area 1
20 *Sep 29 11:59:18.867: End of SPF
21 *Sep 29 11:59:19.367: Generate Changed Type-0x2003 LSA, LSID 10.0.0.4, Seq# 80000002,
Age 3600, Area 1, Prefix 3000:11:22::/64
23 *Sep 29 11:59:20.367: Rcv Changed Type-0x2009 LSA, LSID 10.0.0.0, Adv-Rtr 192.168.0.1,
Seq# 8000769A, Age 2
24 *Sep 29 11:59:20.367: Schedule SPF, Area 0, Change in LSID 10.0.0.0, LSA type P
25 *Sep 29 11:59:20.367: Rcv Changed Type-0x2001 LSA, LSID 10.0.0.0, Adv-Rtr 192.168.0.1,
Seq# 8000769A, Age 2
26 *Sep 29 11:59:20.367: Schedule SPF, Area 0, Change in LSID 10.0.0.0, LSA type R
27 *Sep 29 11:59:20.367: Rcv Changed Type-0x2002 LSA, LSID 10.1.0.1, Adv-Rtr 192.168.0.1,
Seq# 8000769A, Age 2
28 *Sep 29 11:59:20.367: Schedule SPF, Area 0, Change in LSID 10.1.0.1, LSA type N
29 *Sep 29 11:59:20.367: Rcv Changed Type-0x2001 LSA, LSID 10.0.0.0, Adv-Rtr 1.1.1.1, Seq#
 8000769A, Age 2
30 *Sep 29 11:59:20.367: Schedule SPF, Area 0, Change in LSID 10.0.0.0, LSA type R
31 *Sep 29 11:59:20.867: Starting SPF
32 *Sep 29 11:59:20.867: Starting Intra-Area SPF in Area 0
36 *Sep 29 11:59:20.867: Starting Inter-Area SPF in area 0
37 *Sep 29 11:59:20.867: Starting External processing
38 *Sep 29 11:59:20.867: Starting External processing in area 0
39 *Sep 29 11:59:20.867: Starting External processing in area 1
40 *Sep 29 11:59:20.867: End of SPF
```

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

Table 60: show ip ospf Field Descriptions

Field	Description
OSPFv3 Router with ID (10.0.0.1) (Process ID 1)	Process ID and OSPF router ID.
Rcv Changed Type-0x2009 LSA	Description of newly arrived LSA.
LSID	Link-state ID of the LSA.
Adv-Rtr	ID of the advertising router.
Seq#	Link state sequence number (detects old or duplicate link state advertisements).
Age	Link state age (in seconds).
Schedule SPF	Enables SPF to run.
Area	OSPF area ID.
Change in LSID	Changed link-state ID of the LSA.
LSA type	LSA type.

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.

show ipv6 ospf graceful-restart

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
# 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 61: show ipv6 ospf graceful-restart Field Descriptions

Field	Description
Routing Process "ospf 1"	The OSPFv3 routing process ID.
Graceful Restart enabled	The graceful restart feature is enabled on this router.
restart-interval limit: 120 sec	The restart-interval limit.
last restart 00:00:15 ago (took 36 secs)	How long ago the last graceful restart occurred, and how long it took to occur.
Graceful Restart helper support enabled	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.

Field	Description
Router status : Active	This router is in active, as opposed to standby, mode.
Router is running in SSO mode	The router is in stateful switchover mode.
OSPF restart state : NO_RESTART	The current OSPFv3 restart state.
Router ID 10.1.1.1, checkpoint Router ID 10.0.0.0	The IPv6 addresses of the current router and the checkpoint router.

Related Commands

Command	Description
show ipv6 ospf interface	Displays OSPFv3-related interface information.

show ipv6 ospf interface

To display Open Shortest Path First (OSPF)-related interface information, use the **showipv6ospfinterface** command in user EXEC or privileged mode.

show ipv6 ospf [*process-id*] [*area-id*] **interface** [*type number*] [**brief**]

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) Displays information about a specified area only.
type number	(Optional) Interface type and number.
brief	(Optional) Displays brief overview information for OSPF interfaces, states, addresses and masks, and areas on the router.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Examples

show ipv6 ospf interface Standard Output Example

The following is sample output from the **showipv6ospfinterface** command:

```
# 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 3
  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 62: show ipv6 ospf interface Field Descriptions

Field	Description
ATM3/0	Status of the physical link and operational status of protocol.
Link Local Address	Interface IPv6 address.
Area 1, Process ID 1, Instance ID 0, Router ID 172.16.3.3	The area ID, process ID, instance ID, and router ID of the area from which this route is learned.
Network Type POINT_TO_POINT, Cost: 1	Network type and link-state cost.
Transmit Delay	Transmit delay, interface state, and router priority.
Designated Router	Designated router ID and respective interface IP address.
Backup Designated router	Backup designated router ID and respective interface IP address.
Timer intervals configured	Configuration of timer intervals.
Hello	Number of seconds until the next hello packet is sent out this interface.
Neighbor Count	Count of network neighbors and list of adjacent neighbors.

Cisco IOS Release 12.2(33)SRB Example

The following is sample output of the **showipv6ospfinterface** command when the **brief** keyword is entered.

```
# show ipv6 ospf interface brief

Interface    PID   Area            Intf ID    Cost  State Nbrs F/C
VL0          6     0               21         65535 DOWN  0/0
Se3/0        6     0               14         64    P2P   0/0
Lo1          6     0               20         1     LOOP  0/0
Se2/0        6     6               10         62    P2P   0/0
Tu0          1000  0               19         11111 DOWN  0/0
```

OSPF with Authentication on the Interface Example

The following is sample output from the **showipv6ospfinterface** command with authentication enabled on the interface:

```
# 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
  Next 0x0(0)/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 10.11.11.1  (Designated Router)
  Suppress hello for 0 neighbor(s)
```

OSPF with Null Authentication Example

The following is sample output from the **showipv6ospfinterface** command with null authentication configured on the interface:

```
# 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
  Next 0x0(0)/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 10.11.11.1  (Designated Router)
  Suppress hello for 0 neighbor(s)
```

OSPF with Authentication for the Area Example

The following is sample output from the **showipv6ospfinterface** command with authentication configured for the area:

```
# 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
  Next 0x0(0)/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 10.11.11.1  (Designated Router)
  Suppress hello for 0 neighbor(s)
```

OSPF with Dynamic Cost Example

The following display shows sample output from the **showipv6ospfinterface** command when the OSPF cost dynamic is configured.

```
# 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
   Transmit Delay is 1 sec, State POINT_TO_MULTIPOINT,
   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
   Next 0x0(0)/0x0(0)/0x0(0)
   Last flood scan length is 0, maximum is 0
   Last flood scan time is 0 msec, maximum is 0 msec
   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 **showipv6ospfinterface** command when the OSPF graceful restart feature is configured:

```
# 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
  Next 0x0(0)/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 10.1.1.1
  Suppress hello for 0 neighbor(s)
```

Example of an Enabled Protocol

The following display shows that the OSPF interface is enabled for Bidirectional Forwarding Detection (BFD):

```
# 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
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.1.0.1
  Suppress hello for 0 neighbor(s)
```

Related Commands

Command	Description
show ipv6 ospf graceful-restart	Displays OSPFv3 graceful restart information.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
# 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
 Type     LS ID           ADV RTR         Seq NO      Age    Checksum
  1       0.0.0.0         192.168.255.3   0x800000C2  1      0x0014C5
  1       0.0.0.0         192.168.255.2   0x800000C8  0      0x000BCA
  1       0.0.0.0         192.168.255.1   0x800000C5  1      0x008CD1
  2       0.0.0.3         192.168.255.3   0x800000A9  774    0x0058C0
  2       0.0.0.2         192.168.255.3   0x800000B7  1      0x003A63
```

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

Table 63: show ipv6 ospf request-list Field Descriptions

Field	Description
OSPFv3 Router with ID (192.168.255.5) (Process ID 1)	Identification of the router for which information is displayed.
Interface Ethernet0/0	Interface for which information is displayed.
Type	Type of LSA.
LS ID	Link-state ID of the LSA.
ADV RTR	IP address of advertising router.
Seq NO	Sequence number of LSA.
Age	Age of LSA (in seconds).
Checksum	Checksum of LSA.

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

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) Displays information only about a specified area.
neighbor	(Optional) Displays the list of all LSAs waiting to be re-sent for this neighbor.
interface	(Optional) Displays the list of all LSAs waiting to be re-sent on this interface.
interface neighbor	(Optional) Displays the list of all LSAs waiting to be re-sent on this interface, from this neighbor.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
# 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 64: show ipv6 ospf retransmission-list Field Descriptions

Field	Description
OSPFv3 Router with ID (192.168.255.2) (Process ID 1)	Identification of the router for which information is displayed.

Field	Description
Interface Ethernet0/0	Interface for which information is displayed.
Link state retransmission due in	Length of time before next link-state transmission.
Queue length	Number of elements in the retransmission queue.
Type	Type of LSA.
LS ID	Link-state ID of the LSA.
ADV RTR	IP address of advertising router.
Seq NO	Sequence number of the LSA.
Age	Age of LSA (in seconds).
Checksum	Checksum of LSA.

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

detail	(Optional) Displays statistics separately for each OSPF area and includes additional, more detailed statistics.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
# 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):
  SPT    Prefix D-Int  Sum    D-Sum  Ext    D-Ext  Total
  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 X7:0
  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):
  SPT    Prefix D-Int  Sum    D-Sum  Ext    D-Ext  Total
  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 X7:0
  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(P)
```

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

Table 65: show ipv6 ospf statistics Field Descriptions

Field	Description
Area	OSPF area ID.
SPF	Number of SPF algorithms executed in the OSPF area. The number increases by one for each SPF algorithm that is executed in the area.
Executed ago	Time in milliseconds that has passed between the start of the SPF algorithm execution and the current time.
SPF type	SPF type can be Full or Incremental.
SPT	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.
Ext	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.
Total	Total duration time in milliseconds for the SPF algorithm process.
LSIDs processed	Number of LSAs processed during the SPF calculation: • N--Network LSA. • R--Router LSA. • SA--Summary Autonomous System Boundary Router (ASBR) (SA) LSA. • SN--Summary Network (SN) LSA. • Stub--Stub links. • X7--External Type-7 (X7) LSA.

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

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.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
# 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 66: show ipv6 ospf summary-prefix Field Descriptions

Field	Description
OSPFv3 Process	Process ID of the router for which information is displayed.
Metric	Metric used to reach the destination router.
Type	Type of link-state advertisement (LSA).
Tag	LSA tag.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
# 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 67: show ipv6 ospf timers rate-limit Field Descriptions

Field	Description
LSAID	ID of the LSA.
Type	Type of LSA.
Adv Rtr	ID of the advertising router.
Due in:	When the LSA is scheduled to be sent (in hours:minutes:seconds).

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
# 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
```

```
  RX LS req     1                   52
  RX LS upd     4                   320
  RX LS ack     2                   112
  RX Total      16                  852
  TX Failed     0                   0
  TX Hello      8                   304
  TX DB des     3                   144
  TX LS req     1                   52
  TX LS upd     3                   252
  TX LS ack     3                   148
  TX Total      18                  900
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,
    Interface Ethernet0/0
OSPFv3 packets received/sent
  Type          Packets               Bytes
  RX Invalid    0                     0
  RX Hello      6                     240
  RX DB des     3                     144
  RX LS req     1                     52
  RX LS upd     5                     372
  RX LS ack     2                     152
  RX Total      17                    960
  TX Failed     0                     0
  TX Hello      11                    420
  TX DB des     9                     312
  TX LS req     1                     52
  TX LS upd     5                     376
  TX LS ack     3                     148
  TX Total      29                    1308
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
  Type          Packets               Bytes
  RX Invalid    0                     0
  RX Hello      11                    436
  RX DB des     7                     316
  RX LS req     2                     104
  RX LS upd     9                     692
  RX LS ack     4                     264
  RX Total      33                    1812
  TX Failed     0                     0
  TX Hello      19                    724
  TX DB des     12                    456
  TX LS req     2                     104
  TX LS upd     8                     628
  TX LS ack     6                     296
  TX Total      47                    2208
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:

```
# clear ipv6 ospf traffic
```

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

Table 68: show ipv6 ospf traffic Field Descriptions

Field	Description
OSPFv3 statistics	Traffic statistics accumulated for all OSPF processes running on the router. To ensure compatibility with the **showiptraffic** command, only checksum errors are displayed. Identifies the route map name.
OSPFv3 queues statistic for process ID	Queue statistics specific to Cisco IOS software.
Hello queue	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.
Router queue	Statistics for the internal Cisco IOS queue between the OSPF hello process and the OSPF router for all received OSPF packets except OSPF hellos.
queue size	Actual size of the queue.
queue limit	Maximum allowed size of the queue.
queue max size	Maximum recorded size of the queue.
Interface statistics	Per-interface traffic statistics for all interfaces that belong to the specific OSPFv3 process ID.
OSPFv3 packets received/sent	Number of OSPFv3 packets received and sent on the interface, sorted by packet types.
OSPFv3 header errors	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.
OSPFv3 LSA errors	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.
Summary traffic statistics for process ID	Summary traffic statistics accumulated for an OSPFv3 process. **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

Command	Description
clear ip ospf traffic	Clears OSPFv2 traffic statistics.
clear ipv6 ospf traffic	Clears OSPFv3 traffic statistics.
show ip ospf traffic	Displays OSPFv2 traffic statistics.

show ipv6 ospf virtual-links

To display parameters and the current state of Open Shortest Path First (OSPF) virtual links, use the **s how ipv6 ospf virtual-links** command in user EXEC or privileged EXEC mode.

show ipv6 ospf virtual-links

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
# 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 69: show ipv6 ospf virtual-links Field Descriptions

Field	Description
Virtual Link OSPF_VL0 to router 172.16.6.6 is up	Specifies the OSPF neighbor, and if the link to that neighbor is up or down.
Interface ID	Interface ID and IPv6 address of the router.
Transit area 2	The transit area through which the virtual link is formed.
via interface ATM3/0	The interface through which the virtual link is formed.
Cost of using 1	The cost of reaching the OSPF neighbor through the virtual link.
Transmit Delay is 1 sec	The transmit delay (in seconds) on the virtual link.
State POINT_TO_POINT	The state of the OSPF neighbor.

Field	Description
Timer intervals...	The various timer intervals configured for the link.
Hello due in 0:00:06	When the next hello is expected from the neighbor.

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.

```
# 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

rp-address	RP address to be verified.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Examples

```
# show ipv6 pim anycast-rp 110::1:1:1

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

Command	Description
ipv6 pim anycast-RP	Configures the address of the PIM RP for an anycast group range.

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

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
election	Displays BSR state, BSR election, and bootstrap message (BSM)-related timers.
rp-cache	Displays candidate rendezvous point (C-RP) cache learned from unicast C-RP announcements on the elected BSR.
candidate-rp	Displays C-RP state on devices that are configured as C-RPs.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
# 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 70: show ipv6 pim bsr election Field Descriptions

Field	Description
Scope Range List	Scope to which this BSR information applies.

Field	Description
This system is the Bootstrap Router (BSR)	Indicates this device is the BSR and provides information on the parameters associated with it.
BS Timer	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.
This system is candidate BSR	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:

```
# 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.

```
# 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** command used with the **election** keyword would display that information instead.

```
# 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

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
interface-type interface-number	(Optional) Interface type and number. For more information, use the question mark (?) online help function.
rp-address	(Optional) RP IPv6 address.

Command Default

If no interface or RP address is specified, all DFs are displayed.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
# 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:

```
# 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 71: show ipv6 pim df Field Descriptions

Field	Description
Interface	Interface type and number that is configured to run PIM.
DF State	The state of the DF election on the interface. The state can be: • Offer • Winner • Backoff • Lose • None:RP LAN 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.
Timer	DF election timer.
Metrics	Routing metrics to the RP announced by the DF.
RP	The IPv6 address of the RP.

Related Commands

Command	Description
debug ipv6 pim df-election	Displays debug messages for PIM bidirectional DF-election message processing.
ipv6 pim rp-address	Configures the address of a PIM RP for a particular group range.
show ipv6 pim df winner	Displays the DF-election winner on each interface for each RP.

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-namegroup-address*}] | [{*group-rangegroup-mask*}] [**info-source** {**bsr** | **default** | **embedded-rp** | **static**}]}

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.
group-range | *group-mask*	(Optional) Group range list. Includes group ranges with the same prefix or mask length.
info-source	(Optional) Displays all mappings learned from a specific source, such as the bootstrap router (BSR) or static configuration.
bsr	Displays ranges learned through the BSR.
default	Displays ranges enabled by default.
embedded-rp	Displays group ranges learned through the embedded rendezvous point (RP).
static	Displays ranges enabled by static configuration.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
# show ipv6 pim group-map
FF33::/32*
      SSM
      Info source:Static
      Uptime:00:08:32, Groups:0
  FF34::/32*
      SSM
```

```
    Info source:Static
    Uptime:00:09:42, Groups:0
```

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

Table 72: show ipv6 pim group-map Field Descriptions

Field	Description
RP	Address of the RP router if the protocol is sparse mode or bidir.
Protocol	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 (ff[0-f]2::/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 (ff[0-f][0-1]::/16). These addresses are nonroutable, and the router does not need to process them.
Groups	How many groups are present in the topology table from this range.
Info source	Mappings learned from a specific source; in this case, static configuration.
Uptime	The uptime for the group mapping displayed.

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

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
state-on	(Optional) Displays interfaces with PIM enabled.
state-off	(Optional) Displays interfaces with PIM disabled.
type number	(Optional) Interface type and number.

Command Modes

Privileged EXEC (#)

Command History

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

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:

```
# show ipv6 pim interface state-on
Interface          PIM  Nbr   Hello  DR
                        Count Intvl  Prior
Ethernet0          on   0     30     1
    Address:FE80::208:20FF:FE08:D7FF
    DR     :this system
POS1/0             on   0     30     1
    Address:FE80::208:20FF:FE08:D554
    DR     :this system
POS4/0             on   1     30   1
    Address:FE80::208:20FF:FE08:D554
    DR     :FE80::250:E2FF:FE8B:4C80
POS4/1             on   0     30   1
    Address:FE80::208:20FF:FE08:D554
    DR     :this system
Loopback0          on   0     30     1
    Address:FE80::208:20FF:FE08:D554
    DR     :this system
```

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

Table 73: show ipv6 pim interface Field Descriptions

Field	Description
Interface	Interface type and number that is configured to run PIM.
PIM	Whether PIM is enabled on an interface.
Nbr Count	Number of PIM neighbors that have been discovered through this interface.
Hello Intvl	Frequency, in seconds, of PIM hello messages.
DR	IP address of the designated router (DR) on a network.
Address	Interface IP address of the next-hop router.

The following is sample output from the **show ipv6 pim interface** command, modified to display passive interface information:

```
(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 74: show ipv6 pim interface Field Description

Field	Description
PIM	Whether PIM is enabled on an interface. When PIM passive mode is used, a "P" is displayed in the output.

Related Commands

Command	Description
show ipv6 pim neighbor	Displays the PIM neighbors discovered by the Cisco IOS software.

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

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
interface-type	(Optional) Interface type. For more information, use the question mark (**?**) online help function.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
# 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 75: show ipv6 pim join-prune statistics Field Descriptions

Field	Description
Interface	The interface from which the specified packets were transmitted or on which they were received.
Transmitted	The number of packets transmitted on the interface.
Received	The number of packets received on the interface.

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

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
interface	(Optional) Specific interface for which limit information is provided.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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 s PIM interface limit information:

```
# show ipv6 pim limit
```

Related Commands

Command	Description
ipv6 multicast limit	Configures per-interface mroute state limiters in IPv6.
ipv6 multicast limit cost	Applies a cost to mroutes that match per interface mroute state limiters in IPv6.

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

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
detail	(Optional) Displays the additional addresses of the neighbors learned, if any, through the routable address hello option.
interface-type interface-number	(Optional) Interface type and number.
count	(Optional) Displays neighbor counts on each interface.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
# 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 76: show ipv6 pim neighbor Field Descriptions

Field	Description
Neighbor addresses	IPv6 address of the PIM neighbor.
Interface	Interface type and number on which the neighbor is reachable.
Uptime	How long (in hours, minutes, and seconds) the entry has been in the PIM neighbor table.

Field	Description
Expires	How long (in hours, minutes, and seconds) until the entry will be removed from the IPv6 multicast routing table.
DR	Indicates that this neighbor is a designated router (DR) on the LAN.
pri	DR priority used by this neighbor.
Bidir	The neighbor is capable of PIM in bidirectional mode.

Related Commands

Command	Description
show ipv6 pim interfaces	Displays information about interfaces configured for PIM.

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.

show ipv6 pim [**vrf** *vrf-name*] **range-list** [**config**] [{*rp-addressrp-name*}]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
config	(Optional) The client. Displays the range lists configured on the router.
rp-address | *rp-name*	(Optional) The address of a Protocol Independent Multicast (PIM) rendezvous point (RP).

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
# 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:00:03:50
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 77: show ipv6 pim range-list Field Descriptions

Field	Description
config	Config is the client.
SSM	Protocol being used.
FF33::/32	Group range.
Up:	Uptime.

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-addresssource-name*}] | **link-local**}]**route-count** [**detail**]

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.
link-local	(Optional) Displays the link-local groups.
route-count	(Optional) Displays the number of routes in PIM topology table.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
# show ipv6 pim topology
```

```
IP PIM Multicast Topology Table
Entry state:(*/S,G)[RPT/SPT] Protocol Uptime Info
Entry flags:KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive,
    RA - Really Alive, LH - Last Hop, DSS - Don't Signal Sources,
    RR - Register Received, SR - Sending Registers, E - MSDP External,
    DCC - Don't Check Connected
Interface state:Name, Uptime, Fwd, Info
Interface flags:LI - Local Interest, LD - Local Dissinterest,
II - Internal Interest, ID - Internal Dissinterest,
LH - Last Hop, AS - Assert, AB - Admin Boundary
(*,FF05::1)
SM UP:02:26:56 JP:Join(now) Flags:LH
RP:40::1:1:2
RPF:Ethernet1/1,FE81::1
  Ethernet0/1          02:26:56  fwd LI LH
(50::1:1:200,FF05::1)
SM UP:00:00:07 JP:Null(never) Flags:
RPF:Ethernet1/1,FE80::30:1:4
  Ethernet1/1          00:00:07  off LI
```

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

Table 78: show ipv6 pim topology Field Descriptions

Field	Description
Entry flags: KAT	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.
AA, PA	The assume alive (AA) and probe alive (PA) flags are set when the router is in the probe interval for a particular source.
RR	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.
SR	The sending registers (SR) flag is set on the (S, G) entries on the DR as long as it sends registers to the RP.

Related Commands

Command	Description
show ipv6 mrib client	Displays information about the clients of the MRIB.
show ipv6 mrib route	Displays MRIB route information.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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.

```
# 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 79: show ipv6 pim traffic Field Descriptions

Field	Description
Elapsed time since counters cleared	Indicates the amount of time (in hours, minutes, and seconds) since the counters cleared.
Valid PIM Packets	Number of valid PIM packets received and sent.

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 [**vrf** *vrf-name*] **tunnel** [*interface-type interface-number*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
interface-type interface-number	(Optional) Tunnel interface type and number.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
# 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:

```
# 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 80: show ipv6 pim tunnel Field Descriptions

Field	Description
Tunnel0*	Name of the tunnel.

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.

show ipv6 policy

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
# show ipv6 policy

Interface                 Routemap
Ethernet0/0               src-1
```

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

Field	Description
Interface	Interface type and number that is configured to run Protocol-Independent Multicast (PIM).
Routemap	The name of the route map on which IPv6 policy matches were counted.

Related Commands

Command	Description
show route-map	Displays all route maps configured or only the one specified.

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*

Syntax Description

detail | **summary**	(Optional) Displays detailed or summarized information about all IPv6 prefix lists.
list-name	(Optional) The name of a specific IPv6 prefix list.
ipv6-prefix	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.
/ *prefix-length*	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.
longer	(Optional) Displays all entries of an IPv6 prefix list that are more specific than the given *ipv6-prefix* / *prefix-length*values.
first-match	(Optional) Displays the entry of an IPv6 prefix list that matches the given *ipv6-prefix* / *prefix-length*values.
seq *seq-num*	The sequence number of the IPv6 prefix list entry.

Command Default

Displays information about all IPv6 prefix lists.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
# show ipv6 prefix-list detail
ipv6 prefix-list 6to4:
   count: 1, range entries: 0, sequences: 5 - 5, refcount: 2
```

```
   seq 5 permit 2002::/16 (hit count: 313, refcount: 1)
ipv6 prefix-list aggregate:
   count: 2, range entries: 2, sequences: 5 - 10, refcount: 30
   seq 5 deny 3FFE:C00::/24 ge 25 (hit count: 568, refcount: 1)
   seq 10 permit ::/0 le 48 (hit count: 31310, refcount: 1)
```

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

Table 81: show ipv6 prefix-list Field Descriptions

Field	Description
Prefix list with the latest deletion/insertion:	Prefix list that was last modified.
count	Number of entries in the list.
range entries	Number of entries with matching range.
sequences	Sequence number for the prefix entry.
refcount	Number of objects currently using this prefix list.
seq	Entry number in the list.
permit, deny	Granting status.
hit count	Number of matches for the prefix entry.

The following example shows the output of the **show ipv6 prefix-list** command with the **summary** keyword:

```
# show ipv6 prefix-list summary
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
```

Related Commands

Command	Description
clear ipv6 prefix-list	Resets the hit count of the prefix list entries.
distribute-list in	Filters networks received in updates.
distribute-list out	Suppresses networks from being advertised in updates.
ipv6 prefix-list	Creates an entry in an IPv6 prefix list.
ipv6 prefix-list description	Adds a text description of an IPv6 prefix list.
match ipv6 address	Distributes IPv6 routes that have a prefix permitted by a prefix list.
remark (prefix-list)	Adds a comment for an entry in a prefix list.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
# 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 82: show ipv6 protocols Field Descriptions for IS-IS Processes

Field	Description
IPv6 Routing Protocol is	Specifies the IPv6 routing protocol used.
Interfaces	Specifies the interfaces on which the IPv6 IS-IS protocol is configured.
Redistribution	Lists the protocol that is being redistributed.
Inter-area redistribution	Lists the IS-IS levels that are being redistributed into other levels.
using prefix-list	Names the prefix list used in the interarea redistribution.
Address Summarization	Lists all the summary prefixes. If the summary prefix is being advertised, "advertised with metric *x*" will be displayed after the prefix.

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**}]

show ipv6 rip [*name*] [{**database** | **next-hops**}]

Syntax Description

name	(Optional) Name of the RIP process. If the name is not entered, details of all configured RIP processes are displayed.
vrf *vrf-name*	(Optional) Displays information about the specified Virtual Routing and Forwarding (VRF) instance.
database	(Optional) Displays information about entries in the specified RIP IPv6 routing table.
next-hops	(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.

Command Default

Information about all current IPv6 RIP processes is displayed.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Examples

The following is sample output from the **show ipv6 rip** command:

```
# 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
```

```
    Periodic updates 8883, trigger updates 0
  Interfaces:
    None
  Redistribution:
```

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

Table 83: show ipv6 rip Field Descriptions

Field	Description
RIP process	The name of the RIP process.
port	The port that the RIP process is using.
multicast-group	The IPv6 multicast group of which the RIP process is a member.
pid	The process identification number (pid) assigned to the RIP process.
Administrative distance	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.
Updates	The value (in seconds) of the update timer.
expire	The interval (in seconds) in which updates expire.
Holddown	The value (in seconds) of the hold-down timer.
garbage collect	The value (in seconds) of the garbage-collect timer.
Split horizon	The split horizon state is either on or off.
poison reverse	The poison reverse state is either on or off.
Default routes	The origination of a default route into RIP. Default routes are either generated or not generated.
Periodic updates	The number of RIP update packets sent on an update timer.
trigger updates	The number of RIP update packets sent as triggered updates.

The following is sample output from the **show ipv6 rip database** command.

```
# 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::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 84: show ipv6 rip database Field Descriptions

Field	Description
RIP process	The name of the RIP process.
2001:72D:1000::/64	The IPv6 route prefix.
metric	Metric for the route.
installed	Route is installed in the IPv6 routing table.
Ethernet2/2001:DB8:0:ABCD::1	Interface and LL next hop through which the IPv6 route was learned.
expires in	The interval (in seconds) before the route expires.
advertise	For an expired route, the value (in seconds) during which the route will be advertised as expired.
hold	The value (in seconds) of the hold-down timer.
tag	Route tag.

The following is sample output from the **show ipv6 rip next-hops** command.

```
# 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 85: show ipv6 rip next-hops Field Descriptions

Field	Description
RIP process	The name of the RIP process.
2001:DB8:0:1::1/Ethernet4/2	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. **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.
[1 routes]	The number of routes in the IPv6 RIP routing table using the specified next hop.

The following is sample output from the **show ipv6 rip vrf** command:

```
# 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
    Holddown 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 86: show ipv6 rip vrf Field Descriptions

Field	Description
RIP VRF	The name of the RIP VRF.
port	The port that the RIP process is using.
multicast-group	The IPv6 multicast group of which the RIP process is a member.
Administrative distance	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.
Updates	The value (in seconds) of the update timer.
expires after	The interval (in seconds) in which updates expire.
Holddown	The value (in seconds) of the hold-down timer.
garbage collect	The value (in seconds) of the garbage-collect timer.
Split horizon	The split horizon state is either on or off.
poison reverse	The poison reverse state is either on or off.
Default routes	The origination of a default route into RIP. Default routes are either generated or not generated.
Periodic updates	The number of RIP update packets sent on an update timer.
trigger updates	The number of RIP update packets sent as triggered updates.

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 87: show ipv6 rip vrf next-hops Field Descriptions

Field	Description
RIP VRF	The name of the RIP VRF.
metric	Metric for the route.
installed	Route is installed in the IPv6 routing table.
Ethernet0/0/FE80::A8BB:CCFF:FE00:7C00	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. **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:

```
# show ipv6 rip vrf blue database

        RIP VRF "blue", Next Hops
      FE80::A8BB:CCFF:FE00:7C00/Ethernet0/0 [1 paths]
```

Table 88: show ipv6 rip vrf database Field Descriptions

Field	Description
RIP VRF	The name of the RIP VRF.
FE80::A8BB:CCFF:FE00:7C00/Ethernet0/0	Interface and LL next hop through which the IPv6 route was learned.
1 paths	Indicates the number of unique paths to this router that exist in the routing table.

Related Commands

Command	Description
clear ipv6 rip	Deletes routes from the IPv6 RIP routing table.
debug ipv6 rip	Displays the current contents of the IPv6 RIP routing table.
ipv6 rip vrf-mode enable	Enables VRF-aware support for IPv6 RIP.

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

interface -type	(Optional) Specifies the Interface type.
interface -number	(Optional) Specifies the Interface number.
conflicts	(Optional) Displays RAs that differ from the RAs configured for a specified interface.
vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
detail	(Optional) Provides detail about the eligibility of the neighbor for election as the default device.

Command Default

When an interface is not specified, on-link RA information is displayed for all interface types. (The term *onl-ink* refers to a locally reachable address on the link.)

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
# 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 Tunnel57, 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.

```
# show ipv6 routers
```

```
IPV6 ND Routers (table: default)
  Device FE80::100 on Ethernet0/0, last update 0 min
  Hops 64, Lifetime 50 sec, AddrFlag=0, OtherFlag=0, MTU=1500
  HomeAgentFlag=1, Preference=High
  Reachable time 0 msec, Retransmit time 0 msec
  Prefix 2001::100/64 onlink autoconfig
    Valid lifetime 2592000, preferred lifetime 604800
```

The following table describes the significant fields shown in the displays.

Table 89: show ipv6 routers Field Descriptions

Field	Description
Hops	The configured hop limit value for the RA.
Lifetime	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.
AddrFlag	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.
OtherFlag	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.)
MTU	The maximum transmission unit (MTU).
HomeAgentFlag=1	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.
Preference=High	The DRP value, which can be high, medium, or low.
Retransmit time	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.
Prefix	A prefix advertised by the device. Also indicates if on-link or autoconfig bits were set in the RA message.
Valid lifetime	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.
preferred lifetime	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.

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:

```
# 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:

```
# show ipv6 routers conflicts

Device FE80::203:FDFF: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:

```
# 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**}}

Syntax Description

source-vrf	Name or address of the virtual routing and forwarding (VRF) on which lookups are to be performed.
receiver-vrf	Name or address of the VRF in which the lookups originate.
access-list	Name or address of access control list (ACL) to be applied to the group-based VRF selection policy.
vrf	Displays information about the VRF instance.
select	Displays group-to-VRF mapping information.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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], 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:

```
# 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 90: show ipv6 rpf Field Descriptions

Field	Description
RPF information for 2001::1:1:2	Source address that this information concerns.
RPF interface:Ethernet3/2	For the given source, the interface from which the router expects to get packets.
RPF neighbor:FE80::40:1:3	For the given source, the neighbor from which the router expects to get packets.
RPF route/mask:20::/64	Route number and mask that matched against this source.
RPF type:Unicast	Routing table from which this route was obtained, either unicast, or static mroutes.
RPF recursion count	Indicates the number of times the route is recursively resolved.
Metric preference:110	The preference value used for selecting the unicast routing metric to the Route Processor (RP) announced by the designated forwarder (DF).
Metric:30	Unicast routing metric to the RP announced by the DF.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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

```
# 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

Command	Description
ipv6 source-guard attach-policy	Applies IPv6 source guard on an interface.
ipv6 source-guard policy	Defines an IPv6 source-guard policy name and enters source-guard policy configuration mode.

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	Modification
Cisco IOS XE Fuji 16.9.2	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:

```
# 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 91: show ipv6 spd Field Description

Field	Description
Current mode: normal	The current SPD state or mode.
Queue max threshold: 74	The process input queue maximum.

Related Commands

Command	Description
ipv6 spd queue max-threshold	Configures the maximum number of packets in the SPD process input queue.

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

ipv6-address	(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.
ipv6-prefix	(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.
/prefix-length	(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.
interface	(Optional) Name of an interface.
type	(Optional, but required if the **interface** keyword is used) Interface type. For a list of supported interface types, use the question mark (?) online help function.
number	(Optional, but required if the **interface** keyword is used) Interface number. For specific numbering syntax for supported interface types, use the question mark (?) online help function.
recursive	(Optional) Allows the display of recursive static routes only.
detail	(Optional) Specifies the following additional information: • 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.

Command Default

All IPv6 routing information for all active routing tables is displayed.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
# 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 92: show ipv6 static Field Descriptions

Field	Description
via nexthop	Specifies the address of the next in the path to the remote network.
distance 1	Indicates the administrative distance to the specified route.

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:

```
# 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.

```
# 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:

```
# 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.

```
# 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

Command	Description
ipv6 route	Establishes a static IPv6 route.
show ip route	Displays the current state of the routing table.

Command	Description
show ipv6 interface	Displays IPv6 interface information.
show ipv6 route summary	Displays the current contents of the IPv6 routing table in summary format.
show ipv6 tunnel	Displays IPv6 tunnel information.

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*]]

Syntax Description

interface	(Optional) All interfaces. IPv6 forwarding statistics for all interfaces on which IPv6 forwarding statistics are being kept will be displayed.
interface type number	(Optional) Specified interface. Interface statistics that have occurred since the statistics were last cleared on the specific interface are displayed.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
# 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:

```
# 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:

```
# 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
    CEF 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 93: show ipv6 traffic Field Descriptions

Field	Description
source-routed	Number of source-routed packets.

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

name-of-chain	(Optional) Name of the key chain to display, as named in the key chain command.

Command Default

If the command is used without any parameters, then it lists out all the key chains.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Examples

The following is sample output from the **show key chain** command:

```
show key chain
Device# show key chain

Key-chain AuthenticationGLBP:
    key 1 -- text "Thisisasecretkey"
        accept lifetime (always valid) - (always valid) [valid now]
        send lifetime (always valid) - (always valid) [valid now]
Key-chain glbp2:
    key 100 -- text "abc123"
        accept lifetime (always valid) - (always valid) [valid now]
        send lifetime (always valid) - (always valid) [valid now]
```

Related Commands

Command	Description
key-string	Specifies the authentication string for a key.
send-lifetime	Sets the time period during which an authentication key on a key chain is valid to be sent.

show track

To display information about objects that are tracked by the tracking process, use the **show track** command in privileged EXEC mode.

show track [{*object-number* **[brief]** | **application [brief]** | **interface [brief]** | **ip[route [brief]** | **[sla [brief]]** | **ipv6 [route [brief]]** | **list [route [brief]]** | **resolution [ip** | **ipv6]** | **stub-object [brief]** | **summary** | **timers**}]

Syntax Description

object-number	(Optional) Object number that represents the object to be tracked. The range is from 1 to 1000.
brief	(Optional) Displays a single line of information related to the preceding argument or keyword.
application	(Optional) Displays tracked application objects.
interface	(Optional) Displays tracked interface objects.
ip route	(Optional) Displays tracked IP route objects.
ip sla	(Optional) Displays tracked IP SLA objects.
ipv6 route	(Optional) Displays tracked IPv6 route objects.
list	(Optional) Displays the list of boolean objects.
resolution	(Optional) Displays resolution of tracked parameters.
summary	(Optional) Displays the summary of the specified object.
timers	(Optional) Displays polling interval timers.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Use this command to display information about objects that are tracked by the tracking process. When no arguments or keywords are specified, information for all objects is displayed.

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

Examples

The following example shows information about the state of IP routing on the interface that is being tracked:

```
Device# show track 1

Track 1
 Interface GigabitEthernet 1/0/1 ip routing
 IP routing is Down (no IP addr)
  1 change, last change 00:01:08
```

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

Table 94: show track Field Descriptions

Field	Description
Track	Object number that is being tracked.
Interface GigabitEthernet 1/0/1 ip routing	Interface type, interface number, and object that is being tracked.
IP routing is	State value of the object, displayed as Up or Down. If the object is down, the reason is displayed.
1 change, last change	Number of times that the state of a tracked object has changed and the time (in *hh:mm:ss*) since the last change.

Related Commands

Command	Description
show track resolution	Displays the resolution of tracked parameters.
track interface	Configures an interface to be tracked and enters tracking configuration mode.
track ip route	Tracks the state of an IP route and enters tracking configuration mode.

track

To configure an interface to be tracked where the Gateway Load Balancing Protocol (GLBP) weighting changes based on the state of the interface, use the **track** command in global configuration mode. To remove the tracking, use the **no** form of this command.

track *object-number* **interface** *type number* {**line-protocol** | **ip routing** | **ipv6 routing**}
no track *object-number* **interface** *type number* {**line-protocol** | **ip routing** | **ipv6 routing**}

Syntax Description

object-number	Object number in the range from 1 to 1000 representing the interface to be tracked.
interface *type number*	Interface type and number to be tracked.
line-protocol	Tracks whether the interface is up.
ip routing	Tracks whether IP routing is enabled, an IP address is configured on the interface, and the interface state is up, before reporting to GLBP that the interface is up.
ipv6 routing	Tracks whether IPv6 routing is enabled, an IP address is configured on the interface, and the interface state is up, before reporting to GLBP that the interface is up.

Command Default

The state of the interfaces is not tracked.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced..

Usage Guidelines

Use the **track** command in conjunction with the **glbp weighting** and **glbp weighting track** commands to configure parameters for an interface to be tracked. If a tracked interface on a GLBP device goes down, the weighting for that device is reduced. If the weighting falls below a specified minimum, the device will lose its ability to act as an active GLBP virtual forwarder.

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

Examples

In the following example, TenGigabitEthernet interface 0/0/1 tracks whether GigabitEthernet interfaces 1/0/1 and 1/0/3 are up. If either of the GigabitEthernet interface goes down, the GLBP weighting is reduced by the default value of 10. If both GigabitEthernet interfaces go down, the GLBP weighting will fall below the lower threshold and the device will no longer be an active forwarder. To resume its role as an active forwarder, the device must have both tracked interfaces back up, and the weighting must rise above the upper threshold.

```
Device(config)# track 1 interface GigabitEthernet 1/0/1 line-protocol
```

```
Device(config-track)# exit
Device(config)# track 2 interface GigabitEthernet 1/0/3 line-protocol
Device(config-track)# exit
Device(config)# interface TenGigabitEthernet 0/0/1
Device(config-if)# ip address 10.21.8.32 255.255.255.0
Device(config-if)# glbp 10 weighting 110 lower 95 upper 105
Device(config-if)# glbp 10 weighting track 1
Device(config-if)# glbp 10 weighting track 2
```

Related Commands

Command	Description
glbp weighting	Specifies the initial weighting value of a GLBP gateway.
glbp weighting track	Specifies an object to be tracked that affects the weighting of a GLBP gateway.

vrrp

To create a Virtual Router Redundancy Protocol version 3 (VRRPv3) group and enter VRRPv3 group configuration mode, use the **vrrp**. To remove the VRRPv3 group, use the **no** form of this command.

vrrp *group-id* **address-family** {**ipv4** | **ipv6**}
no vrrp *group-id* **address-family** {**ipv4** | **ipv6**}

Syntax Description

group-id	Virtual router group number. The range is from 1 to 255.
address-family	Specifies the address-family for this VRRP group.
ipv4	(Optional) Specifies IPv4 address.
ipv6	(Optional) Specifies IPv6 address.

Command Default

None

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced..

Usage Guidelines

Examples

The following example shows how to create a VRRPv3 group and enter VRRP configuration mode:

```
Device(config-if)# vrrp 3 address-family ipv4
```

Related Commands

Command	Description
timers advertise	Sets the advertisement timer in milliseconds.

vrrp description

To assign a description to the Virtual Router Redundancy Protocol (VRRP) group, use the **vrrp description** command in interface configuration mode. To remove the description, use the **no** form of this command.

description *text*
no description

Syntax Description

text	Text (up to 80 characters) that describes the purpose or use of the group.

Command Default

There is no description of the VRRP group.

Command Modes

VRRP configuration (config-if-vrrp)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Examples

The following example enables VRRP. VRRP group 1 is described as Building A – Marketing and Administration.

```
Device(config-if-vrrp)# description Building A - Marketing and Administration
```

Related Commands

Command	Description
vrrp	Creates a VRRPv3 group and enters VRRPv3 group configuration mode.

vrrp preempt

To configure the device to take over as primary virtual router for a Virtual Router Redundancy Protocol (VRRP) group if it has higher priority than the current primary virtual router, use the **preempt** command in VRRP configuration mode. To disable this function, use the **no** form of this command.

preempt [**delay minimum** *seconds*]
no preempt

Syntax Description

delay minimum *seconds*	(Optional) Number of seconds that the device will delay before issuing an advertisement claiming primary ownership. The default delay is 0 seconds.

Command Default

This command is enabled.

Command Modes

VRRP configuration (config-if-vrrp)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

By default, the device being configured with this command will take over as primary virtual router for the group if it has a higher priority than the current primary 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 primary 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 primary virtual router when its priority of 200 is higher than that of the current primary virtual router. If the device preempts the current primary virtual router, it waits 15 seconds before issuing an advertisement claiming it is the primary virtual router.

```
Device(config-if-vrrp)#preempt delay minimum 15
```

Related Commands

Command	Description
vrrp	Creates a VRRPv3 group and enters VRRPv3 group configuration mode.
priority	Sets the priority level of the device within a VRRP group.

vrrp priority

To set the priority level of the device within a Virtual Router Redundancy Protocol (VRRP) group, use the **priority** command in interface configuration mode. To remove the priority level of the device, use the **no** form of this command.

priority *level*
no priority *level*

Syntax Description

level	Priority of the device within the VRRP group. The range is from 1 to 254. The default is 100.

Command Default

The priority level is set to the default value of 100.

Command Modes

VRRP configuration (config-if-vrrp)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Use this command to control which device becomes the primary virtual router.

Examples

The following example configures the device with a priority of 254:

```
Device(config-if-vrrp)# priority 254
```

Related Commands

Command	Description
vrrp	Creates a VRRPv3 group and enters VRRPv3 group configuration mode.
vrrp preempt	Configures the device to take over as primary virtual router for a VRRP group if it has higher priority than the current primary virtual router.

vrrp timers advertise

To configure the interval between successive advertisements by the primary 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

group	Virtual router group number. The group number range is from 1 to 255.
msec	(Optional) Changes the unit of the advertisement time from seconds to milliseconds. Without this keyword, the advertisement interval is in seconds.
interval	Time interval between successive advertisements by the primary virtual router. The unit of the interval is in seconds, unless the **msec** keyword is specified. The default is 1 second. The valid range is 1 to 255 seconds. When the **msec** keyword is specified, the valid range is 50 to 999 milliseconds.

Command Default

The default interval of 1 second is configured.

Command Modes

VRRP configuration (config-if-vrrp)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The advertisements being sent by the primary virtual router communicate the state and priority of the current primary virtual router.

The **vrrp timers advertise** command configures the time between successive advertisement packets and the time before other routers declare the primary router to be down. Routers or access servers on which timer values are not configured can learn timer values from the primary router. The timers configured on the primary 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 primary.

Examples

The following example shows how to configure the primary virtual router to send advertisements every 4 seconds:

```
Device(config-if-vrrp)# timers advertise 4
```

Related Commands

Command	Description
vrrp	Creates a VRRPv3 group and enters VRRPv3 group configuration mode.

Command	Description
timers learn	Configures the device, when it is acting as backup virtual router for a VRRP group, to learn the advertisement interval used by the primary virtual router.

vrrs leader

To specify a leader's name to be registered with Virtual Router Redundancy Service (VRRS), use the **vrrs leader** command. To remove the specified VRRS leader, use the **no** form of this command.

vrrs leader *vrrs-leader-name*
no vrrs leader *vrrs-leader-name*

Syntax Description

vrrs-leader-name	Name of VRRS Tag to lead.

Command Default

A registered VRRS name is unavailable by default.

Command Modes

VRRP configuration (config-if-vrrp)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Examples

The following example specifies a leader's name to be registered with VRRS:

```
Device(config-if-vrrp)# vrrs leader leader-1
```

Related Commands

Command	Description
vrrp	Creates a VRRP group and enters VRRP configuration mode.

PART V

IP Multicast Routing

• IP Multicast Routing Commands, on page 629

IP Multicast Routing Commands

- clear ip mfib counters, on page 631
- clear ip mroute, on page 632
- clear ip pim snooping vlan, on page 633
- ip igmp filter, on page 634
- ip igmp max-groups, on page 635
- ip igmp profile, on page 637
- ip igmp snooping, on page 638
- ip igmp snooping last-member-query-count, on page 639
- ip igmp snooping querier, on page 641
- ip igmp snooping report-suppression, on page 643
- ip igmp snooping vlan mrouter, on page 644
- ip igmp snooping vlan static, on page 645
- ip multicast auto-enable, on page 646
- ip multicast-routing, on page 647
- ip pim accept-register, on page 648
- ip pim bsr-candidate, on page 649
- ip pim rp-candidate, on page 651
- ip pim send-rp-announce, on page 652
- ip pim snooping, on page 654
- ip pim snooping dr-flood, on page 655
- ip pim snooping vlan, on page 656
- ip pim spt-threshold, on page 657
- match message-type, on page 658
- match service-type, on page 659
- match service-instance, on page 660
- mrinfo, on page 661
- service-policy-query, on page 663
- service-policy, on page 664
- show ip igmp filter, on page 665
- show ip igmp profile, on page 666
- show ip igmp snooping, on page 667
- show ip igmp snooping groups, on page 669
- show ip igmp snooping mrouter, on page 670

- show ip igmp snooping querier, on page 671
- show ip pim autorp, on page 673
- show ip pim bsr-router, on page 674
- show ip pim bsr, on page 675
- show ip pim snooping, on page 676
- show ip pim tunnel, on page 679
- show platform software fed switch ip multicast, on page 681

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Example

The following example shows how to reset all the active MFIB traffic counters for all the multicast tables:

```
# clear ip mfib counters
```

The following example shows how to reset the IP MFIB cache counters to the global default configuration:

```
# clear ip mfib global counters
```

The following example shows how to clear the IP MFIB cache for all the VPN routing and forwarding instances:

```
# clear ip mfib vrf * counters
```

clear ip mroute

To delete the entries in the IP multicast routing table, use the **clear ip mroute**command in privileged EXEC mode.

clear ip mroute [**vrf** *vrf-name*] {***** | *ip-address* | *group-address*} [*hostname* | *source-address*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
*****	Specifies all Multicast routes.
ip-address	Multicast routes for the IP address.
group-address	Multicast routes for the group address.
hostname	(Optional) Multicast routes for the host name.
source-address	(Optional) Multicast routes for the source address.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The *group-address* variable specifies one of the following:

- Name of the multicast group as defined in the DNS hosts table or with the **ip host** command.
- IP address of the multicast group in four-part, dotted notation.

If you specify a group name or address, you can also enter the source argument to specify a name or address of a multicast source that is sending to the group. A source does not need to be a member of the group.

Example

The following example shows how to delete all the entries from the IP multicast routing table:

```
# 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:

```
# 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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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

Command	Description
ip pim snooping	Enables PIM snooping globally.
show ip pim snooping	Displays information about IP PIM snooping.

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 stack or on a standalone . 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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

You can apply IGMP filters only to Layer 2 physical interfaces; you cannot apply IGMP filters to routed ports, switch virtual interfaces (SVIs), or ports that belong to an EtherChannel group.

An IGMP profile can be applied to one or more port interfaces, but one port can have only one profile applied to it.

Example

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 stack or on a standalone . To set the maximum back to the default, which is to have no maximum limit, or to return to the default throttling action, which is to drop the report, use the **no** form of this command.

ip igmp max-groups {*max number* | **action** { **deny** | **replace**} }
no ip igmp max-groups {*max number* | **action**}

Syntax Description

max number	Maximum number of IGMP groups that an interface can join. The range is 0—4294967294. The default is no limit.
action deny	Drops the next IGMP join report when the maximum number of entries is in the IGMP snooping forwarding table. This is the default action.
action replace	Replaces the existing group with the new group for which the IGMP report was received when the maximum number of entries is in the IGMP snooping forwarding table.

Command Default

The default maximum number of groups is no limit.

After the learns the maximum number of IGMP group entries on an interface, the default throttling action is to drop the next IGMP report that the interface receives and to not add an entry for the IGMP group to the interface.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

You can use this command only on Layer 2 physical interfaces and on logical EtherChannel interfaces. You cannot set IGMP maximum groups for routed ports, switch virtual interfaces (SVIs), or ports that belong to an EtherChannel group.

Follow these guidelines when configuring the IGMP throttling action:

- If you configure the throttling action as deny, and set the maximum group limit, the entries that were previously in the forwarding table are not removed, but are aged out. After these entries are aged out, when the maximum number of entries is in the forwarding table, the 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 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:

```
(config)# interface gigabitethernet1/0/2
(config-if)# ip igmp max-groups 25
```

The following example shows how to configure the 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:

```
(config)# interface gigabitethernet2/0/1
(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 stack or on a standalone . From this mode, you can specify the configuration of the IGMP profile to be used for filtering IGMP membership reports from a switch port. To delete the IGMP profile, use the **no** form of this command.

ip igmp profile *profile number*
no ip igmp profile *profile number*

Syntax Description

profile number	The IGMP profile number being configured. The range is from 1—4294967295.

Command Default

No IGMP profiles are defined. When configured, the default action for matching an IGMP profile is to deny matching addresses.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

When you are in IGMP profile configuration mode, you can create a profile by using these commands:

- **deny**—Specifies that matching addresses are denied; this is the default condition.
- **exit**—Exits from igmp-profile configuration mode.
- **no**—Negates a command or resets to its defaults.
- **permit**—Specifies that matching addresses are permitted.
- **range**—Specifies a range of IP addresses for the profile. This can be a single IP address or a range with a start and an end address.

  When entering a range, enter the low IP multicast address, a space, and the high IP multicast address.

You can apply an IGMP profile to one or more Layer 2 interfaces, but each interface can have only one profile applied to it.

Example

The following example shows how to configure IGMP profile 40, which permits the specified range of IP multicast addresses:

```
(config)# ip igmp profile 40
(config-igmp-profile)# permit
(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 or to enable it on a per-VLAN basis, use the **ip igmp snooping** global configuration command on the stack or on a standalone . To return to the default setting, use the **no** form of this command.

ip igmp snooping [**vlan** *vlan-id*]
no ip igmp snooping [**vlan** *vlan-id*]

Syntax Description

vlan *vlan-id*	(Optional) Enables IGMP snooping on the specified VLAN. Ranges are 1—1001 and 1006—4094.

Command Default

IGMP snooping is globally enabled on the .

IGMP snooping is enabled on VLAN interfaces.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

When IGMP snooping is enabled globally, it is enabled in all of the existing VLAN interfaces. When IGMP snooping is globally disabled, it is disabled on all of the existing VLAN interfaces.

VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs, and cannot be used in IGMP snooping.

Example

The following example shows how to globally enable IGMP snooping:

```
(config)# ip igmp snooping
```

The following example shows how to enable IGMP snooping on VLAN 1:

```
(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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

When a multicast host leaves a group, the host sends an IGMP leave message. To check if this host is the last to leave the group, IGMP query messages are sent when the leave message is seen until the **last-member-query-interval** timeout period expires. If no response is received to the last-member queries before the timeout period expires, the group record is deleted.

Use the **ip igmp snooping last-member-query-interval** command to configure the timeout period.

When both IGMP snooping immediate-leave processing and the query count are configured, immediate-leave processing takes precedence.

Note Do not set the count to 1 because the loss of a single packet (the query packet from the to the host or the report packet from the host to the) 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 , 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 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:

```
(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	(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 .

When enabled, the IGMP snooping querier disables itself if it detects IGMP traffic from a multicast router.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Use this command to enable IGMP snooping to detect the IGMP version and IP address of a device that sends IGMP query messages, which is also called a querier.

By default, the IGMP snooping querier is configured to detect devices that use IGMP Version 2 (IGMPv2), but does not detect clients that are using IGMP Version 1 (IGMPv1). You can manually configure the **max-response-time** value when devices use IGMPv2. You cannot configure the max-response-time when devices use IGMPv1. (The value cannot be configured, and is set to zero).

Non-RFC-compliant devices running IGMPv1 might reject IGMP general query messages that have a non-zero value as the **max-response-time** value. If you want the devices to accept the IGMP general query messages, configure the IGMP snooping querier to run IGMPv1.

VLAN IDs 1002—1005 are reserved for Token Ring and FDDI VLANs, and cannot be used in IGMP snooping.

Example

The following example shows how to globally enable the IGMP snooping querier feature:

```
(config)# ip igmp snooping querier
```

The following example shows how to set the IGMP snooping querier maximum response time to 25 seconds:

```
(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:

```
(config)# ip igmp snooping querier query-interval 60
```

The following example shows how to set the IGMP snooping querier TCN query count to 25:

```
(config)# ip igmp snooping querier tcn count 25
```

The following example shows how to set the IGMP snooping querier timeout value to 60 seconds:

```
(config)# ip igmp snooping querier timer expiry 60
```

The following example shows how to set the IGMP snooping querier feature to Version 2:

```
(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 stack or on a standalone . To disable IGMP report suppression, and to forward all IGMP reports to multicast routers, use the **no** form of this command.

ip igmp snooping report-suppression
no ip igmp snooping report-suppression

Syntax Description

This command has no arguments or keywords.

Command Default

IGMP report suppression is enabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

IGMP report suppression is supported only when the multicast query has IGMPv1 and IGMPv2 reports. This feature is not supported when the query includes IGMPv3 reports.

The 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 sends the first IGMP report from all the hosts for a group to all the multicast routers. The 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 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 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:

```
(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 stack or on a standalone . 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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

VLAN IDs 1002—1005 are reserved for Token Ring and FDDI VLANs, and cannot be used in IGMP snooping.

The configuration is saved in NVRAM.

Example

The following example shows how to configure a port as a multicast router port:

```
(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 stack or on a standalone . 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

vlan-id	Enables IGMP snooping on the specified VLAN. Ranges are 1—1001 and 1006—4094.
ip-address	Adds a Layer 2 port as a member of a multicast group with the specified group IP address.
interface *interface-id*	Specifies the interface of the member port. The *interface-id* has these options: • *fastethernet interface number*—A Fast Ethernet IEEE 802.3 interface. • *gigabitethernet interface number*—A Gigabit Ethernet IEEE 802.3z interface. • *tengigabitethernet interface number*—A 10-Gigabit Ethernet IEEE 802.3z interface. • *port-channel interface number*—A channel interface. The range is 0—128.

Command Default

By default, no ports are statically configured as members of a multicast group.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs, and cannot be used in IGMP snooping.

The configuration is saved in NVRAM.

Example

The following example shows how to statically configure a host on an interface:

```
(config)# ip igmp snooping vlan 1 static 224.2.4.12 interface
gigabitEthernet1/0/1

Configuring port gigabitethernet1/0/1 on group 224.2.4.12
```

You can verify your settings by entering the **show ip igmp snooping** command in privileged EXEC mode.

ip multicast auto-enable

To support authentication, authorization, and accounting (AAA) enabling of IP multicast, use the **ip multicast auto-enable** command. This command allows multicast routing to be enabled dynamically on dialup interfaces using AAA attributes from a RADIUS server. To disable IP multicast for AAA, use the **no** form of this command.

ip multicast auto-enable
no ip multicast auto-enable

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Example

The following example shows how to enable AAA on IP multicast:

```
(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*]
no ip multicast-routing [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Enables IP multicast routing for the Multicast VPN routing and forwarding (MVRF) instance specified for the *vrf-name* argument.

Command Default

IP multicast routing is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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

Command	Description
ip pim	Enables PIM on an interface.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Use this command to prevent unauthorized sources from registering with the RP. If an unauthorized source sends a register message to the RP, the RP will immediately send back a register-stop message.

The access list provided for the **ip pim accept-register** command should only filters 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.

```
(config)# ip pim accept-register list ssm-range
(config)# ip access-list extended ssm-range
(config-ext-nacl)# deny ip any 232.0.0.0 0.255.255.255
(config-ext-nacl)# permit ip any any
```

ip pim bsr-candidate

To configure the 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 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 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 is not configured to announce itself as a candidate BSR.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The interface specified for this command must be enabled for Protocol Independent Multicast (PIM) using the **ip pim** command.

This command configures the 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 s 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 always accept and process BSR messages. There is no command to disable this function.

Cisco 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 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:

```
(config)# ip pim bsr-candidate GigabitEthernet1/0/1 0 192
```

ip pim rp-candidate

To configure the 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 as a C-RP, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **rp-candidate** *interface-id* [**group-list** *access-list-number*]
no ip pim [**vrf** *vrf-name*] **rp-candidate** *interface-id* [**group-list** *access-list-number*]

Syntax Description

vrf *vrf-name*	(Optional) Configures the switch to advertise itself to the BSR as PIMv2 C-RP for the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
interface-id	ID of the interface whose associated IP address is advertised as a candidate RP address. Valid interfaces include physical ports, port channels, and VLANs.
group-list *access-list-number*	(Optional) Specifies the standard IP access list number that defines the group prefixes that are advertised in association with the RP address.

Command Default

The is not configured to announce itself to the BSR as a PIMv2 C-RP.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Use this command to configure the to send PIMv2 messages so that it advertises itself as a candidate RP to the BSR.

This command should be configured on backbone s 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.

```
(config)# ip pim rp-candidate GigabitEthernet1/0/1 group-list 4
```

ip pim send-rp-announce

To use Auto-RP to configure groups for which the device will act as a rendezvous point (RP), use the **ip pim send-rp-announce** command in global configuration mode. To unconfigure the device as an RP, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **send-rp-announce** *interface-id* **scope** *ttl-value* [**group-list** *access-list-number*] [**interval** *seconds*]
no ip pim [**vrf** *vrf-name*] **send-rp-announce** *interface-id*

Syntax Description

vrf *vrf-name*	(Optional) Uses Auto-RP to configure groups for which the device will act as a rendezvous point (RP) for the *vrf-name* argument.
interface-id	Enter the interface ID of the interface that identifies the RP address. Valid interfaces include physical ports, port channels, and VLANs.
scope *ttl-value*	Specifies the time-to-live (TTL) value in hops that limits the number of Auto-RP announcements. Enter a hop count that is high enough to ensure that the RP-announce messages reach all the mapping agents in the network. There is no default setting. The range is 1—255.
group-list *access-list-number*	(Optional) Specifies the standard IP access list number that defines the group prefixes that are advertised in association with the RP address. Enter an IP standard access list number from 1—99. If no access list is configured, the RP is used for all groups.
interval *seconds*	(Optional) Specifies the interval between RP announcements, in seconds. The total hold time of the RP announcements is automatically set to three times the value of the interval. The default interval is 60 seconds. The range is 1—16383.

Command Default

Auto-RP is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Enter this command on the device that you want to be an RP. When you are using Auto-RP to distribute group-to-RP mappings, this command causes the router to send an Auto-RP announcement message to the well-known group CISCO-RP-ANNOUNCE (224.0.1.39). This message announces the router as a candidate RP for the groups in the range described by the access list.

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:

```
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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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

Command	Description
clear ip pim snooping	Deletes PIM snooping on an interface.
show ip pim snooping	Displays information about IP PIM snooping.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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 t packets to the designated router:

```
no ip pim snooping dr-flood
```

Related Commands

Command	Description
clear ip pim snooping	Deletes PIM snooping on an interface.
show ip pim snooping	Displays information about IP PIM snooping.

ip pim snooping vlan

To enable Protocol Independent Multicast (PIM) snooping on an interface, use the **ip pim snoopingvlan** 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	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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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

Command	Description
clear ip pim snooping	Deletes PIM snooping on an interface.
ip pim snooping	Enables PIM snooping globally.
show ip pim snooping	Displays information about IP PIM snooping.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Example

The following example shows how to make all the sources for access list 16 use the shared tree:

```
(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 .
any	Allows any match type.
query	Allows only a query from the client for a certain in the network.

Command Default

None

Command Modes

Service list configuration.

Command History

Release	Modification
	This command was introduced.

Usage Guidelines

Multiple service maps of the same name with different sequence numbers can be created, and the evaluation of the filters will be ordered on the sequence number. Service lists are an ordered sequence of individual statements, with each one having a permit or deny result. The evaluation of a service list consists of a list scan in a predetermined order, and an evaluation of the criteria of each statement that matches. A list scan is stopped once the first statement match is found and a permit/deny action associated with the statement match is performed. The default action after scanning through the entire list is to deny.

Note It is not possible to use the **match** command if you have used the **service-list mdns-sd** *service-list-name* **query** command. The **match** command can be used only for the **permit** or **deny** option.

Example

The following example shows how to set the announcement message type to be matched:

```
(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

Release	Modification
	This command was introduced.

Usage Guidelines

It is not possible to use the **match** command if you have used the **service-list mdns-sd** *service-list-name* **query** command. The **match** command can be used only for the **permit** or **deny** option.

Example

The following example shows how to set the value of the mDNS service type string to match:

```
(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

Release	Modification
	This command was introduced.

Usage Guidelines

It is not possible to use the **match** command if you have used the **service-list mdns-sd** *service-list-name* **query** command. The **match** command can be used only for the **permit** or **deny** option.

Example

The following example shows how to set the service instance to match:

```
(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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The **mrinfo** command is the original tool of the multicast backbone (MBONE) to determine which neighboring multicast routers or switches are peering with multicast routers or switches. Cisco routers supports **mrinfo** requests from Cisco IOS Release 10.2.

You can query a multicast router or multilayer switch using the **mrinfo** command. The output format is identical to the multicast routed version of the Distance Vector Multicast Routing Protocol (DVMRP). (The mrouted software is the UNIX software that implements DVMRP.)

Example

The following is the sample output from the **mrinfo** command:

```
# mrinfo
 vrf 192.0.1.0
192.31.7.37 (barrnet-gw.cisco.com) [version cisco 11.1] [flags: PMSA]:
  192.31.7.37 -> 192.31.7.34 (sj-wall-2.cisco.com) [1/0/pim]
  192.31.7.37 -> 192.31.7.47 (dirtylab-gw-2.cisco.com) [1/0/pim]
  192.31.7.37 -> 192.31.7.44 (dirtylab-gw-1.cisco.com) [1/0/pim]
```

Note The flags indicate the following:

- P: prune-capable
- M: mtrace-capable
- S: Simple Network Management Protocol-capable
- A: Auto RP capable

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 service-list-query-periodicity	(Optional) Service-list query periodicity.

Command Default

Disabled.

Command Modes

mDNS configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Since there are devices that do not send unsolicited announcements and to force such devices the learning of services and to keep them refreshed in the cache, this command contains an active query feature that ensures that the services listed in the active query list are queried.

Example

This example shows how to configure service list query periodicity:

```
(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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Example

The following example shows how to apply a filter on incoming service-discovery information on a service list:

```
(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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The **show ip igmp filter** command displays information about all filters defined on the .

Example

The following example shows the sample output from the **show ip igmp filter** command:

```
# show ip igmp filter

IGMP filter enabled
```

show ip igmp profile

To display all the configured Internet Group Management Protocol (IGMP) profiles or a specified IGMP profile, use the **show ip igmp profile** command in privileged EXEC mode.

show ip igmp [**vrf** *vrf-name*] **profile** [*profile number*]

Syntax Description

vrf *vrf-name*	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
profile number	(Optional) IGMP profile number to be displayed. The range is 1 to 4294967295. If no profile number is entered, all the IGMP profiles are displayed.

Command Default

IGMP profiles are undefined by default.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

None

Examples

The following example shows the output of the **show ip igmp profile** command for profile number 40 on the :

```
# 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 :

```
# 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 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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

VLAN IDs 1002—1005 are reserved for Token Ring and FDDI VLANs, and cannot be used in IGMP snooping.

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

Examples

The following is a sample output from the **show ip igmp snooping vlan 1** command. It shows snooping characteristics for a specific VLAN:

```
# 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 :

```
# 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 or the multicast information, use the **show ip igmp snooping groups** command in privileged EXEC mode.

Command Modes

Privileged EXEC

User EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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

Examples

The following is a sample output from the **show ip igmp snooping groups** command without any keywords. It displays the multicast table for the .

```
# show ip igmp snooping groups

Vlan      Group           Type        Version     Port List
------------------------------------------------------------
1         224.1.4.4       igmp                    Gi1/0/11
1         224.1.4.5       igmp                    Gi1/0/11
2         224.0.1.40      igmp        v2          Gi1/0/15
104       224.1.4.2       igmp        v2          Gi2/0/1, Gi2/0/2
104       224.1.4.3       igmp        v2          Gi2/0/1, Gi2/0/2
```

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 .

```
# 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:

```
# show ip igmp snooping groups vlan 104 224.1.4.2

Vlan      Group           Type        Version     Port List
------------------------------------------------------------
104       224.1.4.2       igmp        v2          Gi2/0/1, Gi1/0/15
```

show ip igmp snooping mrouter

To display the Internet Group Management Protocol (IGMP) snooping dynamically learned and manually configured multicast router ports for the 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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

VLAN IDs 1002—1005 are reserved for Token Ring and FDDI VLANs, and cannot be used in IGMP snooping.

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 :

```
# 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 , 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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Use the **show ip igmp snooping querier** command to display the IGMP version and the IP address of a detected device, also called a querier, that sends IGMP query messages. A subnet can have multiple multicast routers but only one IGMP querier. In a subnet running IGMPv2, one of the multicast routers is elected as the querier. The querier can be a Layer 3 .

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 , 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 querier.

The **show ip igmp snooping querier detail** command displays the device IP address most recently detected by the querier and this additional information:

- The elected IGMP querier in the VLAN
- The configuration and operational information pertaining to the 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:

```
> show ip igmp snooping querier
Vlan      IP Address     IGMP Version        Port
-------------------------------------------------
1         172.20.50.11   v3                  Gi1/0/1
2         172.20.40.20   v2                  Router
```

The following is a sample output from the **show ip igmp snooping querier detail** command:

```
> show ip igmp snooping querier detail

Vlan      IP Address     IGMP Version   Port
------------------------------------------------------------
1         1.1.1.1        v2             Fa8/0/1
Global IGMP  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  querier status
-----------------------------------------------------------
elected querier is 1.1.1.1         on port Fa8/0/1
-----------------------------------------------------------
admin state                    : Enabled
admin version                  : 2
source IP address              : 10.1.1.65
query-interval (sec)           : 60
max-response-time (sec)        : 10
querier-timeout (sec)          : 120
tcn query count                : 2
tcn query interval (sec)       : 10
operational state              : Non-Querier
operational version            : 2
tcn query pending count        : 0
```

show ip pim autorp

To display global information about auto-rp, use the **show ip pim autorp** command in privileged EXEC mode.

show ip pim autorp

Syntax Description

This command has no arguments or keywords.

Command Default

Auto RP is enabled by default.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

This command displays whether auto-rp is enabled or disabled.

Example

The following command output shows that Auto RP is enabled:

```
# show ip pim autorp

AutoRP Information:
  AutoRP is enabled.
  RP Discovery packet MTU is 0.
  224.0.1.40 is joined on GigabitEthernet1/0/1.

PIM AutoRP Statistics: Sent/Received
  RP Announce: 0/0, RP Discovery: 0/0
```

show ip pim bsr-router

To display information related to Protocol Independent Multicast (PIM) bootstrap router (BSR) protocol processing, use the **show ip pim bsr-router** command in user EXEC or privileged EXEC mode.

show ip pim bsr-router

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

In addition to Auto RP, the BSR RP method can be configured. After the BSR RP method is configured, this command displays the BSR router information.

The following is sample output from the **show ip pim bsr-router** command:

```
# show ip pim bsr-router

PIMv2 Bootstrap information
This system is the Bootstrap Router (BSR)
  BSR address: 172.16.143.28
  Uptime: 04:37:59, BSR Priority: 4, Hash mask length: 30
  Next bootstrap message in 00:00:03 seconds

Next Cand_RP_advertisement in 00:00:03 seconds.
  RP: 172.16.143.28(Ethernet0), Group acl: 6
```

show ip pim bsr

To display information related to Protocol Independent Multicast (PIM) bootstrap router (BSR) protocol processing, use the **show ip pim bsr** command in user EXEC or privileged EXEC mode.

show ip pim bsr

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

In addition to Auto RP, the BSR RP method can be configured. After the BSR RP method is configured, this command displays the BSR router information.

The following is sample output from the **show ip pim bsr** command:

```
# 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 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-ipgroup-ip*}]}]

Syntax Description

vlan *vlan-id*	Displays information for a specific VLAN; Valid values are from 1—4094.
neighbor	(Optional) Displays information about the neighbor database.
statistics	(Optional) Displays information about the VLAN statistics.
mroute	(Optional) Displays information about the mroute database.
source-ip	(Optional) Source IP address.
group-ip	(Optional) Group IP address.

Command Default

This command has no default settings.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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

IP Address       Mac address     Port            Uptime/Expires    Flags
VLAN 1001: 3 neighbors
10.10.10.2        000a.f330.344a  Po128           02:52:27/00:01:41
10.10.10.1        000a.f330.334a  Hu1/0/7         04:54:14/00:01:38
10.10.10.4        000a.f330.3c00  Hu1/0/1         04:53:45/00:01:34 DR
```

This example shows how to display the detailed statistics for a specific VLAN:

```
Router# show ip pim snooping vlan 1001 statistics

PIMv2 statistics:
Total                                          : 56785
Process Enqueue                                : 56785
Process PIMv2 input queue current outstanding  : 0
Process PIMv2 input queue max size reached     : 110
Error - Global Process State not RUNNING       : 0
Error - Process Enqueue                        : 0
Error - Drops                                  : 0
Error - Bad packet floods                      : 0
Error - IP header generic error                : 0
Error - IP header payload len too long         : 0
Error - IP header payload len too short        : 0
Error - IP header checksum                     : 0
Error - IP header dest ip not 224.0.0.13       : 0
Error - PIM header payload len too short       : 0
Error - PIM header checksum                    : 0
Error - PIM header checksum in Registers       : 0
Error - PIM header version not 2               : 0
```

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
  10.10.10.120->10.10.10.105, 00:14:54/00:02:59, J
  Downstream ports: Po128
  Upstream   ports: Hu1/0/7
  Outgoing   ports: Hu1/0/7 Po128

(11.11.11.10, 225.0.1.0), 00:14:54/00:02:59
  10.10.10.130->10.10.10.120, 00:14:54/00:02:59, SGR-P
  Downstream ports:
  Upstream   ports: Hu1/0/7
  Outgoing   ports:

(*, 225.0.5.0), 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: Hu1/0/7 Po128

(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
```

```
  Downstream ports:
  Upstream   ports: Hu1/0/7
  Outgoing   ports:
Number of matching mroutes found: 4
```

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 95: show ip pim snooping Field Descriptions

Field	Description
Downstream ports	Ports on which PIM joins were received.
Upstream ports	Ports towards RP and source.
Outgoing ports	List of all upstream and downstream ports for the multicast flow.

Related Commands

Command	Description
clear ip pim snooping vlan	Deletes PIM snooping on an interface.
ip pim snooping	Enables PIM snooping globally.
ip pim snooping vlan	Enables PIM snooping on an interface.

show ip pim tunnel

To display information about the Protocol Independent Multicast (PIM) register encapsulation and decapsulation tunnels on an interface, use the **show ip pim tunnel** command.

show ip pim [**vrf** *vrf-name*] **tunnel** [**Tunnel** *interface-number* | **verbose**]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
Tunnel *interface-number*	(Optional) Specifies the tunnel interface number.
verbose	(Optional) Provides additional information, such as the MAC encapsulation header and platform-specific information.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Use the **show ip pim tunnel** to display information about PIM tunnel interfaces.

PIM tunnel interfaces are used by the IPv4 Multicast Forwarding Information Base (MFIB) for the PIM sparse mode (PIM-SM) registration process. Two types of PIM tunnel interfaces are used by the the IPv4 MFIB:

- A PIM encapsulation tunnel (PIM Encap Tunnel)
- A PIM decapsulation tunnel (PIM Decap Tunnel)

The PIM Encap Tunnel is dynamically created whenever a group-to-rendezvous point (RP) mapping is learned (through auto-RP, bootstrap router (BSR), or static RP configuration). The PIM Encap Tunnel is used to encapsulate multicast packets sent by first-hop designated routers (DRs) that have directly connected sources.

Similar to the PIM Encap Tunnel, the PIM Decap Tunnel interface is dynamically created—but it is created only on the RP whenever a group-to-RP mapping is learned. The PIM Decap Tunnel interface is used by the RP to decapsulate PIM register messages.

Note PIM tunnels will not appear in the running configuration.

The following syslog message appears when a PIM tunnel interface is created:

```
* %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel<interface_number>,
changed state to up
```

The following is sample output from the **show ip pim tunnel** taken from an RP. The output is used to verify the PIM Encap and Decap Tunnel on the RP:

```
# 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

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_num* | **active** | **standby** }	The device for which you want to display information. • **active**—Displays information for the active switch. • **standby**—Displays information for the standby switch, if available.
groups	Displays the IP multicast routes per group.
hardware [**detail**]	Displays the IP multicast routes loaded into hardware. The optional **detail** keyword is used to show the port members in the destination index and route index.
interfaces	Displays the IP multicast interfaces.
retry	Displays the IP multicast routes in the retry queue.

Command Modes

Privileged EXEC

Command History

Release	Modification
	This command was introduced.

Usage Guidelines

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

Example

The following example shows how to display platform IP multicast routes per group:

```
# show platform software fed active ip multicast groups

Total Number of entries:3
MROUTE ENTRY vrf 0 (*, 224.0.0.0)
Token: 0x0000001f6  flags:  C
No RPF interface.
Number of OIF: 0
Flags: 0x10   Pkts : 0
OIF Details:No OIF interface.

DI details
----------
Handle:0x603cf7f8 Res-Type:ASIC_RSC_DI Asic-Num:255
Feature-ID:AL_FID_L3_MULTICAST_IPV4 Lkp-ftr-id:LKP_FEAT_INVALID ref_count:1
```

```
Hardware Indices/Handles: index0:0x51f6  index1:0x51f6

Cookie length 56
0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x4 0xe0 0x0 0x0 0x0 0x0 0x0
0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0
0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 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

============================================================

<output truncated>
```

PART VI

Layer 2/3

- Layer 2/3 Commands, on page 685

Layer 2/3 Commands

- channel-group, on page 688
- channel-protocol, on page 691
- clear l2protocol-tunnel counters, on page 692
- clear lacp, on page 693
- clear pagp, on page 694
- clear spanning-tree counters, on page 695
- clear spanning-tree detected-protocols, on page 696
- debug etherchannel, on page 697
- debug lacp, on page 698
- debug pagp, on page 699
- debug platform pm, on page 700
- debug platform udld, on page 701
- debug spanning-tree , on page 702
- instance (VLAN), on page 704
- interface port-channel, on page 706
- l2protocol-tunnel, on page 708
- l2protocol-tunnel cos, on page 711
- lacp max-bundle, on page 712
- lacp port-priority, on page 713
- lacp rate, on page 714
- lacp system-priority, on page 715
- name (MST), on page 716
- pagp learn-method, on page 717
- pagp port-priority, on page 719
- port-channel, on page 720
- port-channel auto, on page 721
- port-channel load-balance, on page 722
- port-channel load-balance extended, on page 724
- port-channel min-links, on page 725
- rep admin vlan, on page 726
- rep block port, on page 727
- rep lsl-age-timer, on page 729
- rep lsl-retries, on page 730

- rep preempt delay, on page 731
- rep preempt segment, on page 732
- rep segment, on page 733
- rep stcn, on page 735
- revision, on page 736
- show dot1q-tunnel, on page 737
- show etherchannel, on page 738
- show interfaces rep detail, on page 741
- show l2protocol-tunnel, on page 742
- show lacp, on page 744
- show pagp, on page 748
- show platform etherchannel, on page 750
- show platform pm, on page 751
- show rep topology, on page 752
- show spanning-tree, on page 754
- show spanning-tree mst, on page 760
- show udld, on page 763
- spanning-tree backbonefast, on page 767
- spanning-tree bpdufilter, on page 768
- spanning-tree bpduguard, on page 770
- spanning-tree bridge assurance, on page 772
- spanning-tree cost, on page 773
- spanning-tree etherchannel guard misconfig, on page 775
- spanning-tree extend system-id, on page 777
- spanning-tree guard, on page 778
- spanning-tree link-type, on page 779
- spanning-tree loopguard default, on page 781
- spanning-tree mode, on page 782
- spanning-tree mst, on page 783
- spanning-tree mst configuration, on page 784
- spanning-tree mst forward-time, on page 786
- spanning-tree mst hello-time, on page 787
- spanning-tree mst max-age, on page 788
- spanning-tree mst max-hops, on page 789
- spanning-tree mst pre-standard, on page 790
- spanning-tree mst priority, on page 792
- spanning-tree mst root, on page 793
- spanning-tree mst simulate pvst global, on page 794
- spanning-tree pathcost method, on page 795
- spanning-tree port-priority, on page 796
- spanning-tree portfast edge bpdufilter default, on page 798
- spanning-tree portfast edge bpduguard default, on page 800
- spanning-tree portfast default, on page 801
- spanning-tree transmit hold-count, on page 803
- spanning-tree uplinkfast, on page 804
- spanning-tree vlan, on page 805

- switchport, on page 808
- switchport access vlan, on page 809
- switchport mode, on page 810
- switchport nonegotiate, on page 812
- switchport voice vlan, on page 813
- udld, on page 816
- udld port, on page 818
- udld reset, on page 820
- vlan dot1q tag native, on page 821

channel-group

To assign an Ethernet port to an EtherChannel group, or to enable an EtherChannel mode, or both, use the **channel-group** command in interface configuration mode. To remove an Ethernet port from an EtherChannel group, use the **no** form of this command.

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

Syntax Description

channel-group-number	Channel group number. The range is 1 to 48.
mode	Specifies the EtherChannel mode.
active	Unconditionally enables Link Aggregation Control Protocol (LACP).
auto	Enables the Port Aggregation Protocol (PAgP) only if a PAgP device is detected.
non-silent	(Optional) Configures the interface for nonsilent operation when connected to a partner that is PAgP-capable. Use in PAgP mode with the **auto** or **desirable** keyword when traffic is expected from the other device.
desirable	Unconditionally enables PAgP.
on	Enables the on mode.
passive	Enables LACP only if a LACP device is detected.

Command Default

No channel groups are assigned.

No mode is configured.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

For Layer 2 EtherChannels, the **channel-group** command automatically creates the port-channel interface when the channel group gets its first physical port. You do not have to use the **interface port-channel** command

in global configuration mode to manually create a port-channel interface. If you create the port-channel interface first, the *channel-group-number* can be the same as the *port-channel-number*, or you can use a new number. If you use a new number, the **channel-group** command dynamically creates a new port channel.

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.

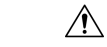
Active mode places a port into a negotiating state in which the port initiates negotiations with other ports by sending LACP packets. A channel is formed with another port group in either the active or passive mode.

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.



Caution Use care when using the on mode. This is a manual configuration, and ports on both ends of the EtherChannel must have the same configuration. If the group is misconfigured, packet loss or spanning-tree loops can occur.

Passive mode places a port into a negotiating state in which the port responds to received LACP packets but does not initiate LACP packet negotiation. A channel is formed only with another port group in active mode.

Do not configure an EtherChannel in both the PAgP and LACP modes. EtherChannel groups running PAgP and LACP can coexist on the same switch or on different switches in the stack (but not in a cross-stack configuration). Individual EtherChannel groups can run either PAgP or LACP, but they cannot interoperate.

If you set the protocol by using the **channel-protocol** interface configuration command, the setting is not overridden by the **channel-group** interface configuration command.

Do not configure a port that is an active or a not-yet-active member of an EtherChannel as an IEEE 802.1x port. If you try to enable IEEE 802.1x authentication on an EtherChannel port, an error message appears, and IEEE 802.1x authentication is not enabled.

Do not configure a secure port as part of an EtherChannel or configure an EtherChannel port as a secure port.

For a complete list of configuration guidelines, see the "Configuring EtherChannels" chapter in the software configuration guide for this release.

Caution Do not 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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Use the **channel-protocol** command only to restrict a channel to LACP or PAgP. If you set the protocol by using the **channel-protocol** command, the setting is not overridden by the **channel-group** 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.

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 l2protocol-tunnel counters

To clear the protocol counters in protocol tunnel ports, use the **clear l2protocol-tunnel counters** command in privileged EXEC mode.

clear l2protocol-tunnel counters [*interface-id*]

Syntax Description

interface-id	(Optional) The interface (physical interface or port cha counters are to be cleared.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

Use this command to clear protocol tunnel counters on the switch or on the specified interface.

This example shows how to clear Layer 2 protocol tunnel counters on an interface:

```
Device# clear l2protocol-tunnel counters gigabitethernet1/0/3
```

clear 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 48.
counters	Clears traffic counters.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

You can clear all counters by using the **clear lacp counters** command, or you can clear only the counters for the specified channel group by using the **clear lacp** *channel-group-number* **counters** command.

This example shows how to clear all channel-group information:

```
Device> 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 48.
counters	Clears traffic counters.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

You can clear all counters by using the **clear pagp counters** command, or you can clear only the counters for the specified channel group by using the **clear pagp** *channel-group-number* **counters** command.

This example shows how to clear all channel-group information:

```
Device> 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*]

Syntax Description

interface *interface-id*	(Optional) Clears all spanning-tree counters on the specified include physical ports, VLANs, and port channels. The VLAN range is 1 to 4094. The port channel range is 1 to 48.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

If the *interface-id* value is not specified, spanning-tree counters are cleared for all interfaces.

This example shows how to clear spanning-tree counters for all interfaces:

```
Device> 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 in channels. The VLAN range is 1 to 4094. The port channel range is 1 to 48.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

A device running the rapid per-VLAN spanning-tree plus (rapid-PVST+) protocol or the Multiple Spanning Tree Protocol (MSTP) supports a built-in protocol migration method that enables it to interoperate with legacy IEEE 802.1D devices. If a rapid-PVST+ or an MSTP device receives a legacy IEEE 802.1D configuration bridge protocol data unit (BPDU) with the protocol version set to 0, the device sends only IEEE 802.1D BPDUs on that port. A multiple spanning-tree (MST) device can also detect that a port is at the boundary of a region when it receives a legacy BPDU, an MST BPDU (Version 3) associated with a different region, or a rapid spanning-tree (RST) BPDU (Version 2).

The device does not automatically revert to the rapid-PVST+ or the MSTP mode if it no longer receives IEEE 802.1D BPDUs because it cannot learn whether the legacy switch has been removed from the link unless the legacy switch is the designated switch. Use the **clear spanning-tree detected-protocols** command in this situation.

This example shows how to restart the protocol migration process on a port:

```
Device> 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.

debug etherchannel [{**all** | **detail** | **error** | **event** | **idb** }]
no debug etherchannel [{**all** | **detail** | **error** | **event** | **idb** }]

Syntax Description

all	(Optional) Displays all EtherChannel debug messages.
detail	(Optional) Displays detailed EtherChannel debug messages.
error	(Optional) Displays EtherChannel error debug messages.
event	(Optional) Displays EtherChannel event messages.
idb	(Optional) Displays PAgP interface descriptor block debug messages.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The **undebug etherchannel** command is the same as the **no debug etherchannel** command.

Note Although the **linecard** keyword is displayed in the command-line help, it is not supported.

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.

debug lacp [{**all** | **event** | **fsm** | **misc** | **packet**}]
no debug lacp [{**all** | **event** | **fsm** | **misc** | **packet**}]

Syntax Description

all	(Optional) Displays all LACP debug messages.
event	(Optional) Displays LACP event debug messages.
fsm	(Optional) Displays messages about changes within the LACP finite state machine.
misc	(Optional) Displays miscellaneous LACP debug messages.
packet	(Optional) Displays the receiving and transmitting LACP control packets.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
Device> enable
Device# debug LACP all
```

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

```
Device> enable
Device# debug LACP event
```

debug pagp

To enable debugging of Port Aggregation Protocol (PAgP) activity, use the **debug pagp** command in privileged EXEC mode. To disable PAgP debugging, use the **no** form of this command.

debug pagp [{**all** | **dual-active** | **event** | **fsm** | **misc** | **packet**}]
no debug pagp [{**all** | **dual-active** | **event** | **fsm** | **misc** | **packet**}]

Syntax Description

all	(Optional) Displays all PAgP debug messages.
dual-active	(Optional) Displays dual-active detection messages.
event	(Optional) Displays PAgP event debug messages.
fsm	(Optional) Displays messages about changes within the PAgP finite state machine.
misc	(Optional) Displays miscellaneous PAgP debug messages.
packet	(Optional) Displays the receiving and transmitting PAgP control packets.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The **undebug pagp** 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.

debug platform pm {**all** | **counters** | **errdisable** | **fec** | **if-numbers** | **l2-control** | **link-status** | **platform** | **pm-vectors** [**detail**] | **ses** | **vlans**}
no debug platform pm {**all** | **counters** | **errdisable** | **fec** | **if-numbers** | **l2-control** | **link-status** | **platform** | **pm-vectors** [**detail**] | **ses** | **vlans**}

Syntax Description

all	Displays all port manager debug messages.
counters	Displays counters for remote procedure call (RPC) debug messages.
errdisable	Displays error-disabled-related events debug messages.
fec	Displays forwarding equivalence class (FEC) platform-related events debug messages.
if-numbers	Displays interface-number translation event debug messages.
l2-control	Displays Layer 2 control infra debug messages.
link-status	Displays interface link-detection event debug messages.
platform	Displays port manager function event debug messages.
pm-vectors	Displays port manager vector-related event debug messages.
detail	(Optional) Displays vector-function details.
ses	Displays service expansion shelf (SES) related event debug messages.
vlans	Displays VLAN creation and deletion event debug messages.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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.

debug platform udld [{**error** | **event**}] [**switch** *switch-number*]
no debug platform udld [{**error** | **event**}] [**switch** *switch-number*]

Syntax Description

error	(Optional) Displays error condition debug messages.
event	(Optional) Displays UDLD-related platform event debug messages.
switch *switch-number*	(Optional) Displays UDLD debug messages for the specified stack member.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The **undebug platform udld** command is the same as the **no debug platform udld** command.

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

debug spanning-tree {**all** | **backbonefast** | **bpdu** | **bpdu-opt** | **config** | **etherchannel** | **events** | **exceptions** | **general** | **ha** | **mstp** | **pvst+** | **root** | **snmp** | **synchronization** | **switch** | **uplinkfast**}
no debug spanning-tree {**all** | **backbonefast** | **bpdu** | **bpdu-opt** | **config** | **etherchannel** | **events** | **exceptions** | **general** | **mstp** | **pvst+** | **root** | **snmp** | **synchronization** | **switch** | **uplinkfast**}

Syntax Description

all	Displays all spanning-tree debug messages.
backbonefast	Displays BackboneFast-event debug messages.
bpdu	Displays spanning-tree bridge protocol data unit (BPDU) debug messages.
bpdu-opt	Displays optimized BPDU handling debug messages.
config	Displays spanning-tree configuration change debug messages.
etherchannel	Displays EtherChannel-support debug messages.
events	Displays spanning-tree topology event debug messages.
exceptions	Displays spanning-tree exception debug messages.
general	Displays general spanning-tree activity debug messages.
ha	Displays high-availability spanning-tree debug messages.
mstp	Debugs Multiple Spanning Tree Protocol (MSTP) events.
pvst+	Displays per-VLAN spanning-tree plus (PVST+) event debug messages.
root	Displays spanning-tree root-event debug messages.
snmp	Displays spanning-tree Simple Network Management Protocol (SNMP) handling debug messages.
switch	Displays switch shim command debug messages. This shim is the software module that is the interface between the generic Spanning Tree Protocol (STP) code and the platform-specific code of various device platforms.
synchronization	Displays the spanning-tree synchronization event debug messages.
uplinkfast	Displays UplinkFast-event debug messages.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The **undebug spanning-tree** command is the same as the **no debug spanning-tree** command.

When you enable debugging on a stack, it is enabled only on the active switch. To enable debugging on the standby switch, start a session from the active switch by using the **session** *switch-number* command in privileged EXEC mode. Enter the **debug** command at the command-line prompt of the standby switch.

To enable debugging on the standby switch without first starting a session on the active switch, use the **remote command** *switch-number LINE* command in privileged EXEC mode.

This example shows how to display all spanning-tree debug messages:

```
Device> enable
Device# debug spanning-tree all
```

instance (VLAN)

To map a VLAN or a group of VLANs to a multiple spanning tree (MST) instance, use the **instance** command in MST configuration mode. To return the VLANs to the default internal spanning tree (CIST) instance, use the **no** form of this command.

instance *instance-id* **vlans** *vlan-range*
no instance *instance-id*

Syntax Description

instance-id	Instance to which the specified VLANs are mapped. The range is from 0 to 4094.
vlans *vlan-range*	Specifies the number of the VLANs to be mapped to the specified instance. The range is from 1 to 4094.

Command Default

No VLANs are mapped to any MST instance (all VLANs are mapped to the CIST instance).

Command Modes

MST configuration mode (config-mst)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The **vlans** *vlan-range* is entered as a single value or a range.

The mapping is incremental, not absolute. When you enter a range of VLANs, this range is added or removed to the existing instances.

Any unmapped VLAN is mapped to the CIST instance.

Examples

The following example shows how to map a range of VLANs to instance 2:

```
Device(config)# spanning-tree mst configuration
Device(config-mst)# instance 2 vlans 1-100
Device(config-mst)#
```

The following example shows how to map a VLAN to instance 5:

```
Device(config)# spanning-tree mst configuration
Device(config-mst)# instance 5 vlans 1100
Device(config-mst)#
```

The following example shows how to move a range of VLANs from instance 2 to the CIST instance:

```
Device(config)# spanning-tree mst configuration
Device(config-mst)# no instance 2 vlans 40-60
Device(config-mst)#
```

The following example shows how to move all the VLANs that are mapped to instance 2 back to the CIST instance:

```
Device(config)# spanning-tree mst configuration
Device(config-mst)# no instance 2
Device(config-mst)#
```

Related Commands

Command	Description
name (MST configuration mode)	Sets the name of an MST region.
revision	Sets the revision number for the MST configuration.
show spanning-tree mst	Displays the information about the MST protocol.
spanning-tree mst configuration	Enters MST configuration mode.

interface port-channel

To access or create a port channel, use the **interface port-channel** command in global configuration mode. Use the **no** form of this command to remove the port channel.

interface port-channel *port-channel-number*
no interface port-channel

Syntax Description

port-channel-number	Channel group number. The range is 1 to 48.

Command Default

No port channel logical interfaces are defined.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

For Layer 2 EtherChannels, you do not have to create a port-channel interface before assigning physical ports to a channel group. Instead, you can use the **channel-group** 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.

l2protocol-tunnel

To enable tunneling of Layer 2 protocols on an access port, IEEE 802.1Q tunnel port, or a port channel, use the **l2protocol-tunnel** command in interface configuration mode on the switch stack or on a standalone switch. Use the **no** form of this command to disable tunneling on the interface.

l2protocol-tunnel [{**drop-threshold** | **shutdown-threshold**}] [*value*] [{**cdp** | **stp** | **vtp** }] [**lldp**] [{**point-to-point** | [{**pagp** | **lacp** | **udld**}]}]
no l2protocol-tunnel [{**drop-threshold** | **shutdown-threshold**}] [*value*] [{**cdp** | **stp** | **vtp** }] [**lldp**] [{**point-to-point** | [{**pagp** | **lacp** | **udld**}]}]

Syntax Description

drop-threshold	(Optional) Sets a drop threshold for the maximum rate of Layer 2 protocol packets per second to be received before an interface drops packets.
shutdown-threshold	(Optional) Sets a shutdown threshold for the maximum rate of Layer 2 protocol packets per second to be received before an interface is shut down.
value	A threshold in packets per second to be received for encapsulation before the interface shuts down, or the threshold before the interface drops packets. The range is 1 to 4096. The default is no threshold.
cdp	(Optional) Enables tunneling of CDP, specifies a shutdown threshold for CDP, or specifies a drop threshold for CDP.
stp	(Optional) Enables tunneling of STP, specifies a shutdown threshold for STP, or specifies a drop threshold for STP.
vtp	(Optional) Enables tunneling or VTP, specifies a shutdown threshold for VTP, or specifies a drop threshold for VTP.
lldp	(Optional) Enables tunneling of LLDP packets.
point-to-point	(Optional) Enables point-to point tunneling of PAgP, LACP, and UDLD packets.
pagp	(Optional) Enables point-to-point tunneling of PAgP, specifies a shutdown threshold for PAgP, or specifies a drop threshold for PAgP.
lacp	(Optional) Enables point-to-point tunneling of LACP, specifies a shutdown threshold for LACP, or specifis a drop threshold for LACP.
udld	(Optional) Enables point-to-point tunneling of UDLD, specifies a shutdown threshold for UDLD, or specifies a drop threshold for UDLD.

Command Default

The default is that no Layer 2 protocol packets are tunneled.

The default is no shutdown threshold for the number of Layer 2 protocol packets.

The default is no drop threshold for the number of Layer 2 protocol packets.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

You can enable tunneling for Cisco Discovery Protocol (CDP), Spanning Tree Protocol (STP), or VLAN Trunking Protocol (VTP) packets. You can also enable point-to-point tunneling for Port Aggregation Protocol (PAgP), Link Aggregation Control Protocol (LACP), or UniDirectional Link Detection (UDLD) packets.

You must enter this command, with or without protocol types, to tunnel Layer 2 packets.

If you enter this command for a port channel, all ports in the channel must have the same configuration.

Layer 2 protocol tunneling across a service-provider network ensures that Layer 2 information is propagated across the network to all customer locations. When protocol tunneling is enabled, protocol packets are encapsulated with a well-known Cisco multicast address for transmission across the network. When the packets reach their destination, the well-known MAC address is replaced by the Layer 2 protocol MAC address.

You can enable Layer 2 protocol tunneling for CDP, STP, and VTP individually or for all three protocols.

In a service-provider network, you can use Layer 2 protocol tunneling to enhance the creation of EtherChannels by emulating a point-to-point network topology. When protocol tunneling is enabled on the service-provider switch for PAgP or LACP, remote customer switches receive the protocol data units (PDUs) and can negotiate automatic creation of EtherChannels.

To enable tunneling of PAgP, LACP, and UDLD packets, you must have a point-to-point network topology. To decrease the link-down detection time, you should also enable UDLD on the interface when you enable tunneling of PAgP or LACP packets.

You can enable point-to-point protocol tunneling for PAgP, LACP, and UDLD individually or for all three protocols.

Caution PAgP, LACP, and UDLD tunneling is only intended to emulate a point-to-point topology. An erroneous configuration that sends tunneled packets to many ports could lead to a network failure.

Enter the **shutdown-threshold** keyword to control the number of protocol packets per second that are received on an interface before it shuts down. When no protocol option is specified with the keyword, the threshold is applied to each of the tunneled Layer 2 protocol types. If you also set a drop threshold on the interface, the shutdown-threshold value must be greater than or equal to the drop-threshold value.

When the shutdown threshold is reached, the interface is error-disabled. If you enable error recovery by entering the **errdisable recovery cause l2ptguard** global configuration command, the interface is brought out of the error-disabled state and allowed to retry the operation again when all the causes have timed out. If the error recovery function is not enabled for **l2ptguard**, the interface stays in the error-disabled state until you enter the **shutdown** and **no shutdown** interface configuration commands.

Enter the **drop-threshold** keyword to control the number of protocol packets per second that are received on an interface before it drops packets. When no protocol option is specified with a keyword, the threshold is applied to each of the tunneled Layer 2 protocol types. If you also set a shutdown threshold on the interface, the drop-threshold value must be less than or equal to the shutdown-threshold value.

When the drop threshold is reached, the interface drops Layer 2 protocol packets until the rate at which they are received is below the drop threshold.

The configuration is saved in NVRAM.

For more information about Layer 2 protocol tunneling, see the software configuration guide for this release.

Examples

This example shows how to enable protocol tunneling for CDP packets and to configure the shutdown threshold as 50 packets per second:

```
Device(config-if)# l2protocol-tunnel cdp
Device(config-if)# l2protocol-tunnel shutdown-threshold cdp 50
```

This example shows how to enable protocol tunneling for STP packets and to configure the drop threshold as 400 packets per second:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet1/0/11
Device(config-if)# l2protocol-tunnel stp
Device(config-if)# l2protocol-tunnel drop-threshold stp 400
```

This example shows how to enable point-to-point protocol tunneling for PAgP and UDLD packets and to configure the PAgP drop threshold as 1000 packets per second:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# switchport access vlan 19
Device(config-if)# switchport mode dot1q-tunnel
Device(config-if)# l2protocol-tunnel point-to-point pagp
Device(config-if)# l2protocol-tunnel point-to-point udld
Device(config-if)# l2protocol-tunnel drop-threshold point-to-point pagp 1000
```

l2protocol-tunnel cos

To configure class of service (CoS) value for all tunneled Layer 2 protocol packets, use the **l2protocol-tunnel cos** global configuration command. To return to the default setting, use the **no** form of this command.

l2protocol-tunnel cos *value*
no l2protocol-tunnel cos

Syntax Description

value	CoS priority value for tunneled Layer 2 protocol packets. If a CoS value is configured for data packets for the interface, the default is to use this CoS value. If no CoS value is configured for the interface, the default is 5. The range is 0 to 7, with 7 being the highest priority.

Command Default

The default is to use the CoS value configured for data on the interface. If no CoS value is configured, the default is 5 for all tunneled Layer 2 protocol packets.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

When enabled, the tunneled Layer 2 protocol packets use this CoS value.

The value is saved in NVRAM.

Examples

This example shows how to configure a Layer-2 protocol-tunnel CoS value of 7:

```
Device> enable
Device# configure terminal
Device(config)# l2protocol-tunnel cos 7
```

lacp max-bundle

To define the maximum number of active LACP ports allowed in a port channel, use the **lacp max-bundle** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

lacp max-bundle *max_bundle_number*
no lacp max-bundle

Syntax Description

max_bundle_number	The maximum number of active LACP ports in the port channel. The range is 1 to 8. The default is 8.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

An LACP channel group can have up to 16 Ethernet ports of the same type. Up to eight ports can be active, and up to eight ports can be in hot-standby mode. When there are more than eight ports in an LACP channel group, the device on the controlling end of the link uses port priorities to determine which ports are bundled into the channel and which ports are put in hot-standby mode. Port priorities on the other device (the noncontrolling end of the link) are ignored.

The **lacp max-bundle** command must specify a number greater than the number specified by the **port-channel min-links** command.

Use the **show etherchannel summary** 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)# lacp max-bundle 5
```

lacp port-priority

To configure the port priority for the Link Aggregation Control Protocol (LACP), use the **lacp port-priority** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

lacp port-priority *priority*
no lacp port-priority

Syntax Description

priority	Port priority for LACP. The range is 1 to 65535.

Command Default

The default is 32768.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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.

Note The LACP port priorities are only effective if the ports are on the device that controls the LACP link. See the **lacp system-priority** 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 **lacp rate** command in interface configuration mode. To return to the default settings, use the **no** form of this command

lacp rate {**normal** | **fast**}
no lacp rate

Syntax Description

normal	Specifies that LACP control packets are ingressed at the normal rate, every 30 seconds after the link is bundled.
fast	Specifies that LACP control packets are ingressed at the fast rate, once every 1 second.

Command Default

The default ingress rate for control packets is 30 seconds after the link is bundled.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Use this command to modify the duration of LACP timeout. The LACP timeout value on Cisco switch is three times the LACP rate that is configured on the interface. Using the **lacp rate**command, you can select the LACP timeout value for a switch to be either 90 seconds or 3 seconds.

This command is supported only on LACP-enabled interfaces.

This example shows how to specify the fast (1 second) ingress rate on interface GigabitEthernet 0/0:

```
Device> 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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The **lacp system-priority** command determines which device in an LACP link controls port priorities.

An LACP channel group can have up to 16 Ethernet ports of the same type. Up to eight ports can be active, and up to eight ports can be in standby mode. When there are more than eight ports in an LACP channel group, the device on the controlling end of the link uses port priorities to determine which ports are bundled into the channel and which ports are put in hot-standby mode. Port priorities on the other device (the noncontrolling end of the link) are ignored.

In priority comparisons, numerically lower values have a higher priority. Therefore, the system with the numerically lower value (higher priority value) for LACP system priority becomes the controlling system. If both devices have the same LACP system priority (for example, they are both configured with the default setting of 32768), the LACP system ID (the device MAC address) determines which device is in control.

The **lacp system-priority** command applies to all LACP EtherChannels on the device.

Use the **show etherchannel summary** 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.

name (MST)

To set the name of a Multiple Spanning Tree (MST) region, use the **name** command in MST configuration submode. To return to the default name, use the **no** form of this command.

name *name*
no name *name*

Syntax Description

name	Name to give the MST region. It can be any string with a maximum length of 32 characters.

Command Modes

MST configuration (config-mst)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Two or more devices with the same VLAN mapping and configuration version number are considered to be in different MST regions if the region names are different.

Note Be careful when using the **name** command to set the name of an MST region. If you make a mistake, you can put the device in a different region. The configuration name is a case-sensitive parameter.

Examples

This example shows how to name a region:

```
Device(config)# spanning-tree mst configuration
Device(config-mst)# name Cisco
Device(config-mst)#
```

Related Commands

Command	Description
instance	Maps a VLAN or a set of VLANs to an MST instance.
revision	Sets the revision number for the MST configuration.
show spanning-tree mst	Displays the information about the MST protocol.
spanning-tree mst configuration	Enters MST configuration submode.

pagp learn-method

To learn the source address of incoming packets received from an EtherChannel port, use the **pagp learn-method** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

pagp learn-method {**aggregation-port** | **physical-port**}
no pagp learn-method

Syntax Description

aggregation-port	Specifies address learning on the logical port channel. The device sends packets to the source using any port in the EtherChannel. This setting is the default. With aggregation-port learning, it is not important on which physical port the packet arrives.
physical-port	Specifies address learning on the physical port within the EtherChannel. The device sends packets to the source using the same port in the EtherChannel from which it learned the source address. The other end of the channel uses the same port in the channel for a particular destination MAC or IP address.

Command Default

The default is aggregation-port (logical port channel).

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The learn method must be configured the same at both ends of the link.

The device supports address learning only on aggregate ports even though the **physical-port** keyword is provided in the command-line interface (CLI). The **pagp learn-method** and the **pagp port-priority** 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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The physical port with the highest priority that is operational and has membership in the same EtherChannel is the one selected for PAgP transmission.

The device supports address learning only on aggregate ports even though the **physical-port** keyword is provided in the command-line interface (CLI). The **pagp learn-method** and the **pagp port-priority** 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.

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 48.
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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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.

port-channel load-balance {**dst-ip** | **dst-mac** | **dst-mixed-ip-port** | **dst-port** | **extended** | **src-dst-ip** | **src-dst-mac** | **src-dst-mixed-ip-port** | **src-dst-port** | **src-ip** | **src-mac** | **src-mixed-ip-port** | **src-port**}

no port-channel load-balance

Syntax Description

dst-ip	Specifies load distribution based on the destination host IP address.
dst-mac	Specifies load distribution based on the destination host MAC address. Packets to the same destination are sent on the same port, but packets to different destinations are sent on different ports in the channel.
dst-mixed-ip-port	Specifies load distribution based on the destination IPv4 or IPv6 address and the TCP/UDP (Layer 4) port number.
dst-port	Specifies load distribution based on the destination TCP/UDP (Layer 4) port number for both IPv4 and IPv6.
extended	Sets extended load balance methods among the ports in the EtherChannel.
src-dst-ip	Specifies load distribution based on the source and destination host IP address.
src-dst-mac	Specifies load distribution based on the source and destination host MAC address.
src-dst-mixed-ip-port	Specifies load distribution based on the source and destination host IP address and TCP/UDP (layer 4) port number.
src-dst-port	Specifies load distribution based on the source and destination TCP/UDP (Layer 4) port number.
src-ip	Specifies load distribution based on the source host IP address.
src-mac	Specifies load distribution based on the source MAC address. Packets from different hosts use different ports in the channel, but packets from the same host use the same port.
src-mixed-ip-port	Specifies load distribution based on the source host IP address and TCP/UDP (Layer 4) port number.
src-port	Specifies load distribution based on the TCP/UDP (Layer 4) port number.

Command Default

The default value is **src-mac**.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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

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

Command	Description
show etherchannel load-balance	Displays information about EtherChannel load balancing.
show running-config	Displays the running configuration.

port-channel load-balance extended

To set combinations of load-distribution methods among the ports in the EtherChannel, use the **port-channel load-balance extended** command in global configuration mode. To reset the extended load-balancing mechanism to the default setting, use the **no** form of this command.

port-channel load-balance extended[{**dst-ip** | **dst-mac** | **dst-port** | **ipv6-label** | **l3-proto** | **src-ip** | **src-mac** | **src-port**}]
no port-channel load-balance extended

Syntax Description

dst-ip	(Optional) Specifies load distribution based on the destination host IP address.
dst-mac	(Optional) Specifies load distribution based on the destination host MAC address. Packets to the same destination are sent on the same port, but packets to different destinations are sent on different ports in the channel.
dst-port	(Optional) Specifies load distribution based on the destination TCP/UDP (Layer 4) port number for both IPv4 and IPv6.
ipv6-label	(Optional) Specifies load distribution based on the source MAC address and IPv6 flow label.
l3-proto	(Optional) Specifies load distribution based on the source MAC address and Layer 3 protocols.
src-ip	(Optional) Specifies load distribution based on the source host IP address.
src-mac	(Optional) Specifies load distribution based on the source MAC address. Packets from different hosts use different ports in the channel, but packets from the same host use the same port.
src-port	(Optional) Specifies load distribution based on the TCP/UDP (Layer 4) port number.

Command Default

The default is **src-mac**.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

An LACP channel group can have up to 16 Ethernet ports of the same type. Up to eight ports can be active, and up to eight ports can be in hot-standby mode. When there are more than eight ports in an LACP channel group, the device on the controlling end of the link uses port priorities to determine which ports are bundled into the channel and which ports are put in hot-standby mode. Port priorities on the other device (the noncontrolling end of the link) are ignored.

The **port-channel min-links** command must specify a number a less than the number specified by the **lacp max-bundle** command.

Use the **show etherchannel summary** 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:

```
Device> enable
Device# configure terminal
Device(config)# interface port-channel 2
Device(config-if)# port-channel min-links 3
```

rep admin vlan

To configure a Resilient Ethernet Protocol (REP) administrative VLAN for 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

vlan-id	48-bit static MAC address.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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

Command	Description
show interfaces rep detail	Displays detailed REP configuration and status for all the interfaces or the specified interface, including the administrative VLAN.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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

Command	Description
show interfaces rep detail	Displays detailed REP configuration and status for all the interfaces or the specified interface, including the administrative VLAN.

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

milliseconds	REP LSL age-out timer value, in milliseconds (ms). The range is from 120 to 10000 in multiples of 40.

Command Default

The default LSL age-out timer value is 5 ms.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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

Command	Description
interface interface-type interface-name	Specifies a physical interface or port channel to receive STCNs.
rep segment	Enables REP on an interface and assigns a segment ID.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced

Usage Guidelines

The **rep lsl-retries** command is used to configure the number of retries before the REP link is disabled. While configuring REP configurable timers, we recommend that you configure the REP LSL number of retries first and then configure the REP LSL age-out timer value.

The following example shows how to configure REP LSL retries.

```
Device> 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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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

Command	Description
rep block port	Configures VLAN load balancing.
show interfaces rep detail	Displays detailed REP configuration and status for all the interfaces or the specified interface, including the administrative VLAN.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Enter this command on the segment, which has the primary edge port on the device.

Ensure that all the other segment configuratios 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

Command	Description
rep block port	Configures VLAN load balancing.
rep preempt delay	Configures a waiting period after a segment port failure and recovery before REP VLAN load balancing is triggered.
show rep topology	Displays REP topology information for a segment or for all the segments.

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]**
no rep segment

Syntax Description

segment-id	Segment for which REP is enabled. Assign a segment ID to the interface. The range is from 1 to 1024.
edge	(Optional) Configures the port as an edge port. Each segment has only two edge ports.
no-neighbor	(Optional) Specifies the segment edge as one with no external REP neighbor.
primary	(Optional) Specifies that the port is the primary edge port where you can configure VLAN load balancing. A segment has only one primary edge port.
preferred	(Optional) Specifies that the port is the preferred alternate port or the preferred port for VLAN load balancing. **Note** Configuring a port as a preferred port does not guarantee that it becomes the alternate port; it merely gives it a slight edge among equal contenders. The alternate port is usually a previously failed port.

Command Default

REP is disabled on the interface.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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
```

revision

To set the revision number for the Multiple Spanning Tree (802.1s) (MST) configuration, use the **revision** command in MST configuration submode. To return to the default settings, use the **no** form of this command.

revision *version*
no revision

Syntax Description

version	Revision number for the configuration; valid values are from 0 to 65535.

Command Default

version is **0**

Command Modes

MST configuration (config-mst)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Devices that have the same configuration but different revision numbers are considered to be part of two different regions.

Note Be careful when using the **revision** command to set the revision number of the MST configuration because a mistake can put the switch in a different region.

Examples

This example shows how to set the revision number of the MST configuration:

```
Device(config)# spanning-tree mst configuration
Device(config-mst)# revision 5
Device(config-mst)#
```

Related Commands

Command	Description
instance	Maps a VLAN or a set of VLANs to an MST instance.
name (MST configuration submode)	Sets the name of an MST region.
show spanning-tree	Displays information about the spanning-tree state.
spanning-tree mst configuration	Enters MST-configuration submode.

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

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Examples

The following are examples of output from the **show dot1q-tunnel** command:

```
Device# show dot1q-tunnel

dot1q-tunnel mode LAN Port(s)
------------------------------
Gi1/0/1
Gi1/0/2
Gi1/0/3
Gi1/0/6
Po2


Device# show dot1q-tunnel interface gigabitethernet1/0/1

dot1q-tunnel mode LAN Port(s)
------------------------------
Gi1/0/1
```

show etherchannel

To display EtherChannel information for a channel, use the **show etherchannel** command in user EXEC mode.

show etherchannel [{*channel-group-number* | {**detail** | **port** | **port-channel** | **protocol** | **summary** }}] | [{**detail** | **load-balance** | **port** | **port-channel** | **protocol** | **summary**}]

Syntax Description

channel-group-number	(Optional) Channel group number. The range is 1 to 48.
detail	(Optional) Displays detailed EtherChannel information.
load-balance	(Optional) Displays the load-balance or frame-distribution scheme among ports in the port channel.
port	(Optional) Displays EtherChannel port information.
port-channel	(Optional) Displays port-channel information.
protocol	(Optional) Displays the protocol that is being used in the channel.
summary	(Optional) Displays a one-line summary per channel group.

Command Modes

User EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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
Channel group = 1        Mode  = Active        Gcchange = -
Port-channel  =          Po1GC = -             Pseudo port-channel = Po1
Port index    =          0Load = 0x00          Protocol = LACP
```

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

Local information:
                        LACP port   Admin   Oper   Port   Port
Port     Flags   State   Priority    Key     Key    Number State
Gi1/0/1   SA      bndl     32768      0x1     0x1    0x101  0x3D
Gi1/0/2    A      bndl     32768      0x0     0x1    0x0    0x3D

Age of the port in the current state: 01d:20h:06m:04s

                  Port-channels in the group:
                  ----------------------

Port-channel: Po1   (Primary Aggregator)

Age of the Port-channel = 01d:20h:20m:26s
Logical slot/port = 10/1          Number of ports = 2
HotStandBy port   = null
Port state        = Port-channel Ag-Inuse
Protocol          = LACP

Ports in the Port-channel:

Index  Load   Port      EC state        No of bits
------+------+------+-----------------+-----------
 0      00    Gi1/0/1    Active           0
 0      00    Gi1/0/2    Active           0

Time since last port bundled:   01d:20h:24m:44s   Gi1/0/2
```

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

```
Device> show etherchannel 1 summary
Flags: D - down P - in port-channel
       I - stand-alone s - suspended
       H - Hot-standby (LACP only)
       R - Layer3 S - Layer2
       u - unsuitable for bundling
       U - in use f - failed to allocate aggregator
       d - default port

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

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------
 1     Po1(SU)       LACP        Gi1/0/1(P) Gi1/0/2(P)
```

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

```
Device> show etherchannel 1 port-channel
Port-channels in the group:
----------------------
Port-channel: Po1 (Primary Aggregator)
------------
Age of the Port-channel = 01d:20h:24m:50s
Logical slot/port = 10/1 Number of ports = 2
Logical slot/port = 10/1 Number of ports = 2
Port state = Port-channel Ag-Inuse
Protocol = LACP
```

```
Ports in the Port-channel:

Index  Load   Port   EC state           No of bits
------+------+------+------------------+-----------
 0      00    Gi1/0/1 Active             0
 0      00    Gi1/0/2 Active             0

Time since last port bundled: 01d:20h:24m:44s Gi1/0/2
```

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

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

show interfaces rep detail

To display detailed 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.

show interfaces [*interface-id*] **rep detail**

Syntax Description

interface-id	(Optional) Physical interface used to display the port ID.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Enter this command on a segment edge port to send STCNs to one or more segments or to an interface.

You can verify your settings by entering the **show interfaces rep detail** 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

Command	Description
rep admin vlan	Configures a REP administrative VLAN for the REP to transmit HFL messages.

show l2protocol-tunnel

To display information about Layer 2 protocol tunnel ports, use the **show l2protocol-tunnel** in EXEC mode.

show l2protocol-tunnel [**interface** *interface-id*] **summary**

Syntax Description

interface *interface-id*	(Optional) Specifies the interface for which protocol tunneling information appears. Valid interfaces are physical ports and port channels. The port-channel range is 1 to 48.
summary	(Optional) Displays only Layer 2 protocol summary information.

Command Default

None

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

After enabling Layer 2 protocol tunneling on an access or IEEE 802.1Q tunnel port by using the **l2protocol-tunnel** interface configuration command, you can configure some or all of these parameters:

- Protocol type to be tunneled
- Shutdown threshold
- Drop threshold

If you enter the **show l2protocol-tunnel interface** command, only information about the active ports on which all the parameters are configured appears.

If you enter the **show l2protocol-tunnel summary** command, only information about the active ports on which some or all of the parameters are configured appears.

Examples

This is an example of output from the **show l2protocol-tunnel** command:

```
Device> show l2protocol-tunnel

COS for Encapsulated Packets: 5
Drop Threshold for Encapsulated Packets: 0

Port        Protocol Shutdown  Drop      Encapsulation Decapsulation Drop
                     Threshold Threshold Counter       Counter       Counter
---------- -------- --------- --------- ------------- ------------- -------------
Gi3/0/3     ---           ----      ----          ----          ----          ----
            ---           ----      ----          ----          ----          ----
            ---           ----      ----          ----          ----          ----
            pagp          ----      ----             0        242500
            lacp          ----      ----         24268        242640
            udld          ----      ----             0        897960
```

```
Gi3/0/4    ---          ----      ----         ----         ----         ----
           ---          ----      ----         ----         ----         ----
           ---          ----      ----         ----         ----         ----
           pagp         1000      ----        24249        242700
           lacp         ----      ----        24256        242660
           udld         ----      ----            0        897960
Gi6/0/1    cdp          ----      ----       134482       1344820
           ---          ----      ----         ----         ----         ----
           ---          ----      ----         ----         ----         ----
           pagp         1000      ----            0        242500
           lacp          500      ----            0        485320
           udld          300      ----        44899        448980
Gi6/0/2     cdp          ----      ----       134482       1344820
           ---          ----      ----         ----         ----         ----
           ---          ----      ----         ----         ----         ----
           pagp         ----      1000            0        242700
           lacp         ----      ----            0        485220
           udld          300      ----        44899        448980
```

This is an example of output from the **show l2protocol-tunnel summary** command:

```
Device> show l2protocol-tunnel summary

COS for Encapsulated Packets: 5
Drop Threshold for Encapsulated Packets: 0

Port    Protocol       Shutdown         Drop             Status
                       Threshold        Threshold
                       (cdp/stp/vtp)    (cdp/stp/vtp)
                       (pagp/lacp/udld) (pagp/lacp/udld)
------- -------------  ---------------- ---------------- ----------
Gi3/0/2 pagp lacp udld  ----/----/----   ----/----/----   up
Gi4/0/3 pagp lacp udld  1000/ 500/----   ----/----/----   up
Gi9/0/1 pagp ---- ----  ----/----/----   1000/----/----   down
Gi9/0/2 pagp ---- ----  ----/----/----   1000/----/----   down
```

show 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 48.
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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

You can enter any **show lacp** command to display the active channel-group information. To display specific channel information, enter the **show lacp** command with a channel-group number.

If you do not specify a channel group, information for all channel groups appears.

You can enter the *channel-group-number* to specify a channel group for all keywords except **sys-id**.

This is an example of output from the **show lacp counters** user EXEC command. The table that follows describes the fields in the display.

```
Device> show lacp counters
               LACPDUs         Marker     Marker Response   LACPDUs
Port         Sent  Recv     Sent  Recv     Sent  Recv     Pkts  Err
--------------------------------------------------------------------
Channel group:1
Gi2/0/1       19    10        0    0         0    0        0
Gi2/0/2       14    6         0    0         0    0        0
```

Table 96: show lacp counters Field Descriptions

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

Field	Description
Marker Response Sent and Recv	The number of LACP marker response packets sent and received by a port.
LACPDUs Pkts and Err	The number of unknown and illegal packets received by LACP for a port.

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

```
Device> show lacp 1 internal
Flags:  S - Device is requesting Slow LACPDUs
        F - Device is requesting Fast LACPDUs
        A - Device is in Active mode       P - Device is in Passive mode

Channel group 1
                            LACP port    Admin    Oper    Port     Port
Port      Flags   State     Priority     Key      Key     Number   State
Gi2/0/1    SA      bndl      32768         0x3      0x3       0x4    0x3D
Gi2/0/2    SA      bndl      32768         0x3      0x3       0x5    0x3D
```

The following table describes the fields in the display:

Table 97: show lacp internal Field Descriptions

Field	Description
State	State of the specific port. These are the allowed values: • **–** —Port is in an unknown state. • **bndl**—Port is attached to an aggregator and bundled with other ports. • **susp**—Port is in a suspended state; it is not attached to any aggregator. • **hot-sby**—Port is in a hot-standby state. • **indiv**—Port is incapable of bundling with any other port. • **indep**—Port is in an independent state (not bundled but able to handle data traffic. In this case, LACP is not running on the partner port). • **down**—Port is down.
LACP Port Priority	Port priority setting. LACP uses the port priority to put ports in standby mode when there is a hardware limitation that prevents all compatible ports from aggregating.

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:

          Partner               Partner              Partner
Port      System ID             Port Number   Age    Flags
Gi2/0/1   32768,0007.eb49.5e80   0xC             19s    SP

          LACP Partner          Partner       Partner
          Port Priority         Oper Key      Port State
          32768                 0x3           0x3C

Partner's information:
```

```
          Partner                 Partner                 Partner
Port      System ID               Port Number   Age       Flags
Gi2/0/2   32768,0007.eb49.5e80    0xD             15s     SP

          LACP Partner            Partner       Partner
          Port Priority           Oper Key      Port State
          32768                   0x3           0x3C
```

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

```
Device> show lacp sys-id
32765,0002.4b29.3a00
```

The system identification is made up of the system priority and the system MAC address. The first two bytes are the system priority, and the last six bytes are the globally administered individual MAC address associated to the system.

show pagp

To display Port Aggregation Protocol (PAgP) channel-group information, use the **show pagp** command in EXEC mode.

show pagp [*channel-group-number*] {**counters** | **dual-active** | **internal** | **neighbor**}

Syntax Description

channel-group-number	(Optional) Channel group number. The range is 1 to 48.
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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

You can enter any **show pagp** command to display the active channel-group information. To display the nonactive information, enter the **show pagp** command with a channel-group number.

Examples

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

```
Device> show pagp 1 counters
             Information        Flush
Port         Sent   Recv     Sent   Recv
---------------------------------------
Channel group: 1
  Gi1/0/1    45     42       0      0
  Gi1/0/2    45     41       0      0
```

This is an example of output from the **show pagp dual-active** command:

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

Channel group 1
          Dual-Active     Partner             Partner   Partner
Port      Detect Capable  Name                Port      Version
Gi1/0/1   No              -p2                 Gi3/0/3   N/A
Gi1/0/2   No              -p2                 Gi3/0/4   N/A

<output truncated>
```

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

```
Device> show pagp 1 internal
Flags:  S - Device is sending Slow hello.  C - Device is in Consistent state.
        A - Device is in Auto mode.
Timers: H - Hello timer is running.        Q - Quit timer is running.
        S - Switching timer is running.    I - Interface timer is running.

Channel group 1
                               Hello    Partner  PAgP     Learning  Group
Port        Flags State   Timers  Interval Count   Priority   Method  Ifindex
Gi1/0/1     SC    U6/S7   H       30s      1        128        Any      16
Gi1/0/2     SC    U6/S7   H       30s      1        128        Any      16
```

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

```
Device> show pagp 1 neighbor

Flags:  S - Device is sending Slow hello.  C - Device is in Consistent state.
        A - Device is in Auto mode.        P - Device learns on physical port.

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

show platform etherchannel

To display platform-dependent EtherChannel information, use the **show platform etherchannel** command in privileged EXEC mode.

show platform etherchannel *channel-group-number* {**group-mask** | **load-balance mac** *src-mac dst-mac* [**ip** *src-ip dst-ip* [**port** *src-port dst-port*]]} [**switch** *switch-number*]

Syntax Description

channel-group-number	Channel group number. The range is 1 to 48.
group-mask	Displays EtherChannel group mask.
load-balance	Tests EtherChannel load-balance hash algorithm.
mac *src-mac dst-mac*	Specifies the source and destination MAC addresses.
ip *src-ip dst-ip*	(Optional) Specifies the source and destination IP addresses.
port *src-port dst-port*	(Optional) Specifies the source and destination layer port numbers.
switch *switch-number*	(Optional) Specifies the stack member.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Use this command only when you are working directly with a technical support representative while troubleshooting a problem.

Do not use this command unless a technical support representative asks you to do so.

show platform pm

To display platform-dependent port manager information, use the **show platform pm** command in privileged EXEC mode.

show platform pm {**etherchannel** *channel-group-number* **group-mask** | **interface-numbers** | **port-data** *interface-id* | **port-state**}

Syntax Description

etherchannel *channel-group-number* **group-mask**	Displays the EtherChannel group-mask table for the specified channel group. The range is 1 to 48.
interface-numbers	Displays interface numbers information.
port-data *interface-id*	Displays port data information for the specified interface.
port-state	Displays port state information.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Use this command only when you are working directly with your technical support representative while troubleshooting a problem.

Do not use this command unless your technical support representative asks you to do so.

show rep topology

To display 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

segment *segment-id*	(Optional) Specifies the segment for which to display the REP topology information. The *segment-id* range is from 1 to 1024.
archive	(Optional) Displays the previous topology of the segment. This keyword is useful for troubleshooting a link failure.
detail	(Optional) Displays detailed REP topology information.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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
```

```
  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 spanning-tree

To display spanning-tree information for the specified spanning-tree instances, use the **show spanning-tree** command in privileged EXEC mode.

show spanning-tree [*bridge-group*] [{ **active** | **backbonefast** | **blockedports** | **bridge** [*id*] | **detail** | **inconsistentports** | **instances** | **interface** *interface-type interface-number* | **mst** [{ *list* | **configuration** [**digest**] }] | **pathcost method** | **root** | **summary** [**totals**] | **uplinkfast** | **vlan** *vlan-id* }]

Syntax Description

bridge-group	(Optional) Specifies the bridge group number. The range is 1 to 255.
active	(Optional) Displays spanning-tree information on active interfaces only.
backbonefast	(Optional) Displays spanning-tree BackboneFast status.
blockedports	(Optional) Displays blocked port information.
bridge	(Optional) Displays status and configuration of this switch.
detail	(Optional) Shows status and configuration details.
inconsistentports	(Optional) Displays information about inconsistent ports.
instances	(Optional) Displays information about maximum STP instances.
interface *interface-type interface-number*	(Optional) Specifies the type and number of the interface. Enter each interface designator, using a space to separate it from the one before and the one after. Ranges are not supported. Valid interfaces include physical ports and virtual LANs (VLANs). See the “Usage Guidelines” for valid values.
mst	(Optional) Specifies multiple spanning-tree.
list	(Optional) Specifies a multiple spanning-tree instance list.
configuration digest	(Optional) Displays the multiple spanning-tree current region configuration.
pathcost *method*	(Optional) Displays the default path-cost calculation method that is used. See the “Usage Guidelines” section for the valid values.
root	(Optional) Displays root-switch status and configuration.
summary	(Optional) Specifies a summary of port states.
totals	(Optional) Displays the total lines of the spanning-tree state section.
uplinkfast	(Optional) Displays spanning-tree UplinkFast status.
vlan *vlan-id*	(Optional) Specifies the VLAN ID. The range is 1 to 4094. If the *vlan-id* value is omitted, the command applies to the spanning-tree instance for all VLANs.
id	(Optional) Identifies the spanning tree bridge.

port-channel *number*	(Optional) Identifies the Ethernet channel associated with the interfaces.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The keywords and arguments that are available with the **show spanning-tree** command vary depending on the platform you are using and the network modules that are installed and operational.

The **port-channel** *number* values from 257 to 282 are supported on the Content Switching Module (CSM) and the Firewall Services Module (FWSM) only.

The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 2 to 13 and valid values for the port number are from 1 to 48.

When checking spanning tree-active states and you have a large number of VLANs, you can enter the **show spanning-tree summary total** command. You can display the total number of VLANs without having to scroll through the list of VLANs.

The valid values for keyword **pathcoast** *method* are:

- **append**: Appends the redirected output to a URL (supporting the append operation).
- **begin**: Begins with the matching line.
- **exclude**: Excludes matching lines.
- **include**: Includes matching lines.
- **redirect**: Redirects output to a URL.
- **tee**: Copies output to a URL.

When you run the **show spanning-tree** command for a VLAN or an interface the switch router will display the different port states for the VLAN or interface. The valid spanning-tree port states are listening, learning, forwarding, blocking, disabled, and loopback.

```
Device#
show spanning-tree
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    32769
             Address     5c71.0dfe.8380
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     5c71.0dfe.8380
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec
```

```
Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi1/0/1             Desg FWD 20000     128.1    P2p
Gi1/0/18            Desg FWD 20000     128.18   P2p
Gi1/0/21            Desg FWD 20000     128.21   P2p
Te1/0/25            Desg FWD 20000     128.25   P2p
Te1/0/37            Desg FWD 2000      128.37   P2p
Te1/0/38            Desg FWD 2000      128.38   P2p
Te1/0/45            Desg FWD 20000     128.45   P2p
Te1/0/48            Desg FWD 20000     128.48   P2p
```

See the table below for definitions of the port states:

Table 98: show spanning-tree vlan Command Port States

Field	Definition
BLK	Blocked is when the port is still sending and listening to BPDU packets but is not forwarding traffic.
DIS	Disabled is when the port is not sending or listening to BPDU packets and is not forwarding traffic.
FWD	Forwarding is when the port is sending and listening to BPDU packets and forwarding traffic.
LBK	Loopback is when the port recieves its own BPDU packet back.
LIS	Listening is when the port spanning tree initially starts to listen for BPDU packets for the root bridge.
LRN	Learning is when the port sets the proposal bit on the BPDU packets it sends out

This example shows how to display a summary of interface information:

```
Device#
show spanning-tree
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    32769
             Address     6cb2.ae4a.4fc0
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     6cb2.ae4a.4fc0
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Fif1/0/17           Desg FWD 2000      128.17   P2p
Fif1/0/19           Desg FWD 800       128.19   P2p
Fif1/0/21           Desg FWD 2000      128.21   P2p
Fif1/0/23           Desg FWD 2000      128.23   P2p
TwoH1/0/42          Desg FWD 500       128.42   P2p
Fou1/0/44           Desg FWD 50        128.44   P2p
Fif2/0/17           Back BLK 2000      128.185  P2p
Fif2/0/19           Back BLK 800       128.187  P2p
Fif2/0/21           Back BLK 2000      128.189  P2p
Fif2/0/23           Back BLK 2000      128.191  P2p
Fou2/0/43           Desg FWD 50        128.211  P2p
Fou2/0/44           Back BLK 50        128.212  P2p
Hu5/0/13            Desg FWD 500       128.685  P2p
```

```
Hu5/0/15            Desg FWD 500       128.687  P2p
Hu5/0/21            Back BLK 500       128.693  P2p
Hu5/0/23            Back BLK 500       128.695  P2p
Fou6/0/27           Back BLK 50        128.867  P2p
Hu6/0/29            Desg FWD 200       128.869  P2p
Hu6/0/30            Back BLK 200       128.870  P2p
```

The table below describes the fields that are shown in the example.

Table 99: show spanning-tree Command Output Fields

Field	Definition
Port ID Prio.Nbr	Port ID and priority number.
Cost	Port cost.
Sts	Status information.

This example shows how to display information about the spanning tree for this bridge only:

```
Device# show spanning-tree bridge

                                                    Hello  Max  Fwd
Vlan                         Bridge ID               Time  Age  Dly  Protocol
---------------- ---------------------------------- -----  ---  ---  --------
VLAN0001         32769 (32768,   1) 5c71.0dfe.8380    2    20   15  rstp
```

This example shows how to display detailed information about the interface:

```
Device#
show spanning-tree detail
 VLAN0001 is executing the rstp compatible Spanning Tree protocol
  Bridge Identifier has priority 32768, sysid 1, address 5c71.0dfe.8380
  Configured hello time 2, max age 20, forward delay 15, transmit hold-count 6
  We are the root of the spanning tree
  Topology change flag not set, detected flag not set
  Number of topology changes 27 last change occurred 4d19h ago
          from TenGigabitEthernet1/0/48
  Times:  hold 1, topology change 35, notification 2
          hello 2, max age 20, forward delay 15
  Timers: hello 0, topology change 0, notification 0, aging 300

 Port 1 (GigabitEthernet1/0/1) of VLAN0001 is designated forwarding
   Port path cost 20000, Port priority 128, Port Identifier 128.1.
   Designated root has priority 32769, address 5c71.0dfe.8380
   Designated bridge has priority 32769, address 5c71.0dfe.8380
   Designated port id is 128.1, designated path cost 0
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   Link type is point-to-point by default
   BPDU: sent 208695, received 1

 Port 18 (GigabitEthernet1/0/18) of VLAN0001 is designated forwarding
!
!
<<output truncated>>
```

This example shows how to display a summary of port states:

```
Device#
```

```
show spanning-tree summary
Switch is in rapid-pvst mode
Root bridge for: VLAN0001
Extended system ID                       is enabled
Portfast Default                         is disabled
PortFast BPDU Guard Default             is disabled
Portfast BPDU Filter Default            is disabled
Loopguard Default                       is disabled
EtherChannel misconfig guard             is enabled
UplinkFast                               is disabled
BackboneFast                             is enabled but inactive in rapid-pvst mode
Configured Pathcost method used is long

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
VLAN0001                    1         0        0         26         27
---------------------- -------- --------- -------- ---------- ----------
1 vlan                      1         0        0         26         27
```

This example shows how to display the total lines of the spanning-tree state section:

```
Device#
show spanning-tree summary total Switch is in rapid-pvst mode
Root bridge for: VLAN0001
Extended system ID                       is enabled
Portfast Default                         is disabled
PortFast BPDU Guard Default             is disabled
Portfast BPDU Filter Default            is disabled
Loopguard Default                       is disabled
EtherChannel misconfig guard             is enabled
UplinkFast                               is disabled
BackboneFast                             is enabled but inactive in rapid-pvst mode
Configured Pathcost method used is long

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
1 vlan                      1         0        0         26         27
```

This example shows how to display information about the spanning tree for a specific VLAN:

```
Device#
show spanning-tree vlan 200
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    32769
             Address     5c71.0dfe.8380
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     5c71.0dfe.8380
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi1/0/1             Desg FWD 20000     128.1    P2p
Gi1/0/18            Desg FWD 20000     128.18   P2p
Gi1/0/21            Desg FWD 20000     128.21   P2p
Te1/0/25            Desg FWD 20000     128.25   P2p
Te1/0/37            Desg FWD 2000      128.37   P2p
Te1/0/38            Desg FWD 2000      128.38   P2p
Te1/0/45            Desg FWD 20000     128.45   P2p
```

```
Te1/0/48            Desg FWD 20000     128.48   P2p
!
!
<<output truncated>>
```

The table below describes the fields that are shown in the example.

Table 100: show spanning-tree vlan Command Output Fields

Field	Definition
Role	Current 802.1w role; valid values are Boun (boundary), Desg (designated), Root, Altn (alternate), and Back (backup).
Sts	Spanning-tree states; valid values are BKN* (broken)[1], BLK (blocking), DWN (down), LTN (listening), LBK (loopback), LRN (learning), and FWD (forwarding).
Cost	Port cost.
Prio.Nbr	Port ID that consists of the port priority and the port number.
Status	Status information; valid values are as follows: • P2p/Shr: The interface is considered as a point-to-point (resp. shared) interface by the spanning tree. • Edge: PortFast has been configured (either globally using the **default**command or directly on the interface) and no BPDU has been received. • *ROOT_Inc, *LOOP_Inc, *PVID_Inc and *TYPE_Inc: The port is in a broken state (BKN*) for an inconsistency. The port would be (respectively) Root inconsistent, Loopguard inconsistent, PVID inconsistent, or Type inconsistent. • Bound(type): When in MST mode, identifies the boundary ports and specifies the type of the neighbor (STP, RSTP, or PVST). • Peer(STP): When in PVRST rapid-pvst mode, identifies the port connected to a previous version of the 802.1D bridge.

[1] For information on the *, see the definition for the Status field.

show spanning-tree mst

To display the information about the Multiple Spanning Tree (MST) protocol, use the **show spanning-tree mst** command in privileged EXEC mode.

show spanning-tree mst [{ **configuration** [**digest**] | *instance-id-number* }] [**interface** *interface*] [**detail**] [**service instance**]

Syntax Description

instance-id-number	(Optional) Instance identification number. The range is from 0 to 4094.
detail	(Optional) Displays detailed information about the MST protocol.
interface	(Optional) Displays the information about the interfaces. See the "Usage Guidelines" section for valid number values.
configuration	(Optional) Displays information about the region configuration.
digest	(Optional) Displays information about the message digest 5 (MD5) algorithm included in the current MST configuration identifier (MSTCI).
interface	(Optional) Displays information about the interface type.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The valid values for the *interface* argument depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 2 to 13 and valid values for the port number are from 1 to 48.

The number of valid values for **port-channel** *number* are a maximum of 64 values ranging from 1 to 282. The **port-channel** *number* values from 257 to 282 are supported on the Content Switching Module (CSM) and the Firewall Services Module (FWSM) only.

The number of valid values for **vlan** are from 1 to 4094.

In the output display of the **show spanning-tree mst configuration** command, a warning message may be displayed. This message appears if you do not map secondary VLANs to the same instance as the associated primary VLAN. The display includes a list of the secondary VLANs that are not mapped to the same instance as the associated primary VLAN. The warning message is as follows:

```
These secondary vlans are not mapped to the same instance as their primary:
-> 3
```

In the output display of the **show spanning-tree mst configuration digest** command, if the output applies to both standard and prestandard bridges at the same time on a per-port basis, two different digests are displayed.

If you configure a port to transmit prestandard PortFast bridge protocol data units (BPDUs) only, the prestandard flag displays in the **show spanning-tree** commands. The variations of the prestandard flag are as follows:

- Pre-STD (or pre-standard in long format): This flag is displayed if the port is configured to transmit prestandard BPDUs and if a prestandard neighbor bridge has been detected on this interface.
- Pre-STD-Cf (or pre-standard (config) in long format): This flag is displayed if the port is configured to transmit prestandard BPDUs but a prestandard BPDU has not been received on the port, the autodetection mechanism has failed, or a misconfiguration, if there is no prestandard neighbor, has occurred.
- Pre-STD-Rx (or prestandard (rcvd) in long format): This flag is displayed when a prestandard BPDU has been received on the port, but it has not been configured to send prestandard BPDUs. The port will send prestandard BPDUs, but Cisco recommends that you change the port configuration so that the interaction with the prestandard neighbor does not rely only on the autodetection mechanism.

If the configuration is not prestandard compliant (for example, a single MST instance has an ID that is greater than or equal to 16,) the prestandard digest is not computed and the following output is displayed:

```
Device# show spanning-tree mst configuration digest

Name      [region1]
Revision  2     Instances configured 3
Digest          0x3C60DBF24B03EBF09C5922F456D18A03
Pre-std Digest  N/A, configuration not pre-standard compatible
```

MST BPDUs include an MSTCI that consists of the region name, region revision, and an MD5 digest of the VLAN-to-instance mapping of the MST configuration.

See the **show spanning-tree mst** command field description table for output descriptions.

Examples

The following example shows how to display information about the region configuration:

```
Device# show spanning-tree mst configuration

Name      [train]
Revision  2702
Instance  Vlans mapped
--------  ---------------------------------------------------------------------
0         1-9,11-19,21-29,31-39,41-4094
1         10,20,30,40
---------------------------------------------------------------------------
```

The following example shows how to display additional MST-protocol values:

```
Device# show spanning-tree mst 3 detail

###### MST03 vlans mapped: 3,3000-3999
Bridge address 0002.172c.f400 priority 32771 (32768 sysid 3)
Root this switch for MST03
GigabitEthernet1/1 of MST03 is boundary forwarding
Port info port id 128.1 priority 128
cost 20000
Designated root address 0002.172c.f400 priority 32771
cost 0
Designated bridge address 0002.172c.f400 priority 32771 port
id 128.1
Timers: message expires in 0 sec, forward delay 0, forward transitions 1
Bpdus (MRecords) sent 4, received 0
FastEthernet4/1 of MST03 is designated forwarding
Port info port id 128.193 priority 128 cost
200000
Designated root address 0002.172c.f400 priority 32771
```

```
cost 0
Designated bridge address 0002.172c.f400 priority 32771 port id
128.193
Timers: message expires in 0 sec, forward delay 0, forward transitions 1
Bpdus (MRecords) sent 254, received 1
FastEthernet4/2 of MST03 is backup blocking
Port info port id 128.194 priority 128 cost
200000
Designated root address 0002.172c.f400 priority 32771
cost 0
Designated bridge address 0002.172c.f400 priority 32771 port id
128.193
Timers: message expires in 2 sec, forward delay 0, forward transitions 1
Bpdus (MRecords) sent 3, received 252
```

The following example shows how to display the MD5 digest included in the current MSTCI:

```
Device# show spanning-tree mst configuration digest

Name      [mst-config]
Revision  10    Instances configured 25
Digest          0x40D5ECA178C657835C83BBCB16723192
Pre-std Digest  0x27BF112A75B72781ED928D9EC5BB4251
```

Related Commands

Command	Description
spanning-tree mst	Sets the path cost and port-priority parameters for any MST instance.
spanning-tree mst forward-time	Sets the forward-delay timer for all the instances on the Cisco 7600 series router.
spanning-tree mst hello-time	Sets the hello-time delay timer for all the instances on the Cisco 7600 series router.
spanning-tree mst max-hops	Specifies the number of possible hops in the region before a BPDU is discarded.

show udld

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

show udld [**Auto-Template** | **Capwap** | **GigabitEthernet** | **GroupVI** | **InternalInterface** | **Loopback** | **Null** | **Port-channel** | **TenGigabitEthernet** | **Tunnel** | **Vlan**] *interface_number*
show udld neighbors

Syntax Description

Auto-Template	(Optional) Displays UDLD operational status of the auto-template interface. The range is from 1 to 999.
Capwap	(Optional) Displays UDLD operational status of the CAPWAP interface. The range is from 0 to 2147483647.
GigabitEthernet	(Optional) Displays UDLD operational status of the GigabitEthernet interface. The range is from 0 to 9.
GroupVI	(Optional) Displays UDLD operational status of the group virtual interface. The range is from 1 to 255.
InternalInterface	(Optional) Displays UDLD operational status of the internal interface. The range is from 0 to 9.
Loopback	(Optional) Displays UDLD operational status of the loopback interface. The range is from 0 to 2147483647.
Null	(Optional) Displays UDLD operational status of the null interface.
Port-channel	(Optional) Displays UDLD operational status of the Ethernet channel interfaces. The range is 1 to 48.
TenGigabitEthernet	(Optional) Displays UDLD operational status of the Ten Gigabit Ethernet interface. The range is from 0 to 9.
Tunnel	(Optional) Displays UDLD operational status of the tunnel interface. The range is from 0 to 2147483647.
Vlan	(Optional) Displays UDLD operational status of the VLAN interface. The range is from 1 to 4095.
interface-id	(Optional) ID of the interface and port number. Valid interfaces include physical ports, VLANs, and port channels.
neighbors	(Optional) Displays neighbor information only.

Command Modes

User EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

If you do not enter an interface ID, administrative and operational UDLD status for all interfaces appear.

This is an example of output from the **show udld** *interface-id* command. For this display, UDLD is enabled on both ends of the link, and UDLD detects that the link is bidirectional. The table that follows describes the fields in this display.

```
Device> show udld gigabitethernet2/0/1
Interface gi2/0/1
---
Port enable administrative configuration setting: Follows device default
Port enable operational state: Enabled
Current bidirectional state: Bidirectional
Current operational state: Advertisement - Single Neighbor detected
Message interval: 60
Time out interval: 5
Entry 1
Expiration time: 146
Device ID: 1
Current neighbor state: Bidirectional
Device name: Switch-A
Port ID: Gi2/0/1
Neighbor echo 1 device: Switch-B
Neighbor echo 1 port: Gi2/0/2
Message interval: 5
CDP Device name: Switch-A
```

Table 101: show udld Field Descriptions

Field	Description
Interface	The interface on the local device configured for UDLD.
Port enable administrative configuration setting	How UDLD is configured on the port. If UDLD is enabled or disabled, the port enable configuration setting is the same as the operational enable state. Otherwise, the enable operational setting depends on the global enable setting.
Port enable operational state	Operational state that shows whether UDLD is actually running on this port.
Current bidirectional state	The bidirectional state of the link. An unknown state appears if the link is down or if it is connected to an UDLD-incapable device. A bidirectional state appears if the link is a normal two-way connection to a UDLD-capable device. All other values mean miswiring.

Field	Description
Current operational state	The current phase of the UDLD state machine. For a normal bidirectional link, the state machine is most often in the Advertisement phase.
Message interval	How often advertisement messages are sent from the local device. Measured in seconds.
Time out interval	The time period, in seconds, that UDLD waits for echoes from a neighbor device during the detection window.
Entry 1	Information from the first cache entry, which contains a copy of echo information received from the neighbor.
Expiration time	The amount of time in seconds remaining before this cache entry is aged out.
Device ID	The neighbor device identification.
Current neighbor state	The neighbor's current state. If both the local and neighbor devices are running UDLD normally, the neighbor state and local state should be bidirectional. If the link is down or the neighbor is not UDLD-capable, no cache entries appear.
Device name	The device name or the system serial number of the neighbor. The system serial number appears if the device name is not set or is set to the default (Switch).
Port ID	The neighbor port ID enabled for UDLD.
Neighbor echo 1 device	The device name of the neighbors' neighbor from which the echo originated.
Neighbor echo 1 port	The port number ID of the neighbor from which the echo originated.
Message interval	The rate, in seconds, at which the neighbor is sending advertisement messages.
CDP device name	The CDP device name or the system serial number. The system serial number appears if the device name is not set or is set to the default (Switch).

This is an example of output from the **show udld neighbors** command:

```
Device> enable
Device# show udld neighbors
Port     Device Name          Device ID  Port-ID  OperState
-------- -------------------- ---------- -------- --------------
Gi2/0/1  Switch-A             1          Gi2/0/1  Bidirectional
```

```
Gi3/0/1  Switch-A            2          Gi3/0/1  Bidirectional
```

spanning-tree backbonefast

To enable BackboneFast to allow a blocked port on a switch to change immediately to a listening mode, use the **spanning-tree backbonefast** command in global configuration mode. To return to the default setting, use the **no** form of this command.

spanning-tree backbonefast
no spanning-tree backbonefast

Syntax Description

This command has no arguments or keywords.

Command Default

BackboneFast is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

BackboneFast should be enabled on all of the Cisco devices containing an Ethernet switch network module. BackboneFast provides for fast convergence in the network backbone after a spanning-tree topology change. It enables the switch to detect an indirect link failure and to start the spanning-tree reconfiguration sooner than it would under normal spanning-tree rules.

Use the **show spanning-tree** privileged EXEC command to verify your settings.

Examples

The following example shows how to enable BackboneFast on the device:

```
Device(config)# spanning-tree backbonefast
```

Related Commands

Command	Description
show spanning-tree	Displays information about the spanning-tree state.

spanning-tree bpdufilter

To enable bridge protocol data unit (BPDU) filtering on the interface, use the **spanning-tree bpdufilter** command in interface configuration or template configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree bpdufilter { **enable** | **disable** }
no spanning-tree bpdufilter

Syntax Description

enable	Enables BPDU filtering on this interface.
disable	Disables BPDU filtering on this interface.

Command Default

The setting that is already configured when you enter the **spanning-tree portfast edge bpdufilter default** command .

Command Modes

Interface configuration (config-if)

Template configuration (config-template)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Caution Be careful when you enter the **spanning-tree bpdufilter enable** command. Enabling BPDU filtering on an interface is similar to disabling the spanning tree for this interface. If you do not use this command correctly, you might create bridging loops.

Entering the **spanning-tree bpdufilter enable** command to enable BPDU filtering overrides the PortFast configuration.

When configuring Layer 2-protocol tunneling on all the service-provider edge switches, you must enable spanning-tree BPDU filtering on the 802.1Q tunnel ports by entering the **spanning-tree bpdufilter enable** command.

BPDU filtering prevents a port from sending and receiving BPDUs. The configuration is applicable to the whole interface, whether it is trunking or not. This command has three states:

- **spanning-tree bpdufilter enable**: Unconditionally enables BPDU filtering on the interface.
- **spanning-tree bpdufilter disable**: Unconditionally disables BPDU filtering on the interface.
- **no spanning-tree bpdufilter**: Enables BPDU filtering on the interface if the interface is in operational PortFast state and if you configure the **spanning-tree portfast bpdufilter default** command.

Use the **spanning-tree portfast bpdufilter default** command to enable BPDU filtering on all ports that are already configured for PortFast.

Examples

This example shows how to enable BPDU filtering on this interface:

```
Device(config-if)# spanning-tree bpdufilter enable
Device(config-if)#
```

The following example shows how to enable BPDU filtering on an interface using interface template:

```
Device# configure terminal
Device(config)# template user-template1
Device(config-template)# spanning-tree bpdufilter enable
Device(config-template)# end
```

Related Commands

Command	Description
show spanning-tree	Displays information about the spanning-tree state.
spanning-tree portfast edge bpdufilter default	Enables BPDU filtering by default on all PortFast ports.

spanning-tree bpduguard

To enable bridge protocol data unit (BPDU) guard on the interface, use the **spanning-tree bpduguard** command in interface configuration and template configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree bpduguard { **enable** | **disable** }
no spanning-tree bpduguard

Syntax Description

enable	Enables BPDU guard on this interface.
disable	Disables BPDU guard on this interface.

Command Modes

Interface configuration (config-if)

Template configuration (config-template)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

BPDU guard prevents a port from receiving BPDUs. Typically, this feature is used in a service-provider environment where the network administrator wants to prevent an access port from participating in the spanning tree. If the port still receives a BPDU, it is put in the error-disabled state as a protective measure. This command has three states:

- **spanning-tree bpduguard enable**: Unconditionally enables BPDU guard on the interface.
- **spanning-tree bpduguard disable**: Unconditionally disables BPDU guard on the interface.
- **no spanning-tree bpduguard**: E nables BPDU guard on the interface if it is in the operational PortFast state and if the **spanning-tree portfast bpduguard default** command is configured.

Examples

This example shows how to enable BPDU guard on this interface:

```
Device(config-if)# spanning-tree bpduguard enable
Device(config-if)#
```

The following example shows how to enable BPDU guard on an interface using interface template:

```
Device# configure terminal
Device(config)# template user-template1
Device(config-template)# spanning-tree bpduguard enable
Device(config-template)# end
```

Related Commands

Command	Description
show spanning-tree	Displays information about the spanning-tree state.

Command	Description
spanning-tree portfast edge bpduguard default	Enables BPDU guard by default on all PortFast ports.

spanning-tree bridge assurance

To enable bridge assurance on all network ports on the device, use the **spanning-tree bridge assurance** command in global configuration mode. To disable bridge assurance, use the **no** form of this command.

spanning-tree bridge assurance
no spanning-tree bridge assurance

Syntax Description

This command has no arguments or keywords.

Command Default

Bridge assurance is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Bridge assurance protects against a unidirectional link failure or other software failure and a device that continues to forward data traffic when it is no longer running the spanning tree algorithm.

Bridge assurance is enabled only on spanning tree network ports that are point-to-point links. Both ends of the link must have bridge assurance enabled. If the device on one side of the link has bridge assurance enabled and the device on the other side either does not support bridge assurance or does not have this feature enabled, the connecting port is blocked.

Disabling bridge assurance causes all configured network ports to behave as normal spanning tree ports.

Examples

This example shows how to enable bridge assurance on all network ports on the switch:

```
Device(config)#
spanning-tree bridge assurance
Device(config)#
```

This example shows how to disable bridge assurance on all network ports on the switch:

```
Device(config)#
no spanning-tree bridge assurance
Device(config)#
```

Related Commands

Command	Description
show spanning-tree	Displays information about the spanning-tree state.

spanning-tree cost

To set the path cost of the interface for Spanning Tree Protocol (STP) calculations, use the **spanning-tree cost** command in interface configuration or template configuration mode. To revert to the default value, use the **no** form of this command.

spanning-tree cost *cost*
no spanning-tree cost

Syntax Description

cost	Path cost. The range is from 1 to 200000000.

Command Modes

Interface configuration (config-if)

Template configuration (config-template)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

When you specify a value for the cost argument, higher values indicate higher costs. This range applies regardless of the protocol type specified.

If a loop occurs, spanning tree uses the path cost when selecting an interface to place into the forwarding state. A lower path cost represents higher-speed transmission.

Examples

The following example shows how to access an interface and set a path cost value of 250 for the spanning tree VLAN associated with that interface:

```
Router(config)# interface ethernet 2/0
Router(config-if)# spanning-tree cost 250
```

The following example shows how to set a path cost value of 250 for the spanning tree VLAN associated with an interface using an interface template:

```
Device# configure terminal
Device(config)# template user-template1
Device(config-template)# spanning-tree cost 250
Device(config-template)# end
```

Related Commands

Command	Description
show spanning-tree	Displays spanning-tree information for the specified spanning-tree instances.
spanning-tree port-priority	Sets an interface priority when two bridges tie for position as the root bridge.

Command	Description
spanning-tree portfast (global)	Enables PortFast mode, where the interface is immediately put into the forwarding state upon linkup without waiting for the timer to expire.
spanning-tree portfast (interface)	Enables PortFast mode, where the interface is immediately put into the forwarding state upon linkup without waiting for the timer to expire.
spanning-tree uplinkfast	Enables the UplinkFast feature.
spanning-tree vlan	Configures STP on a per-VLAN basis.

spanning-tree etherchannel guard misconfig

To display an error message when a loop due to a channel misconfiguration is detected, use the **spanning-tree etherchannel guard misconfig** command in global configuration mode. To disable the error message, use the **no** form of this command.

spanning-tree etherchannel guard misconfig
no spanning-tree etherchannel guard misconfig

Syntax Description

This command has no arguments or keywords.

Command Default

Error messages are displayed.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

EtherChannel uses either Port Aggregation Protocol (PAgP) or Link Aggregation Control Protocol (LACP) and does not work if the EtherChannel mode of the interface is enabled using the **channel-group** group-number mode on command.

The **spanning-tree etherchannel guard misconfig** command detects two types of errors: misconfiguration and misconnection errors. A misconfiguration error is an error between the port-channel and an individual port. A misconnection error is an error between a device that is channeling more ports and a device that is not using enough Spanning Tree Protocol (STP) Bridge Protocol Data Units (BPDUs) to detect the error. In this case, the device will only error disable an EtherChannel if the switch is a nonroot device.

When an EtherChannel-guard misconfiguration is detected, this error message displays:

```
msgdef(CHNL_MISCFG, SPANTREE, LOG_CRIT, 0, "Detected loop due to etherchannel misconfiguration
 of %s %s")
```

To determine which local ports are involved in the misconfiguration, enter the **show interfaces status err-disabled** command. To check the EtherChannel configuration on the remote device, enter the **show etherchannel summary** command on the remote device.

After you correct the configuration, enter the **shutdown** and the **no shutdown** commands on the associated port-channel interface.

Examples

This example shows how to enable the EtherChannel-guard misconfiguration:

```
Device(config)# spanning-tree etherchannel guard misconfig
 Device(config)#
```

Related Commands

Command	Description
show etherchannel summary	Displays the EtherChannel information for a channel.

Command	Description
show interfaces status err-disabled	Displays the interface status or a list of interfaces in an error-disabled state on LAN ports only.
shutdown	Disables an interface.

spanning-tree extend system-id

To enable the extended-system ID feature on chassis that support 1024 MAC addresses, use the **spanning-tree extend system-id** command in global configuration mode. To disable the extended system identification, use the **no** form of this command.

spanning-tree extend system-id
no spanning-tree extend system-id

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled on systems that do not provide 1024 MAC addresses.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Enabling or disabling the extended-system ID updates the bridge IDs of all active Spanning Tree Protocol (STP) instances, which might change the spanning-tree topology.

Examples

This example shows how to enable the extended-system ID:

```
Device(config)# spanning-tree extend system-id
Device(config)#
```

Related Commands

Command	Description
show spanning-tree	Displays information about the spanning-tree state.

spanning-tree guard

To enable or disable the guard mode, use the **spanning-tree guard** command in interface configuration and template configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree guard { **loop** | **root** | **none** }
no spanning-tree guard

Syntax Description

loop	Enables the loop-guard mode on the interface.
root	Enables root-guard mode on the interface.
none	Sets the guard mode to none.

Command Default

Guard mode is disabled.

Command Modes

Interface configuration (config-if)

Template configuration (config-template)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Examples

This example shows how to enable root guard:

```
Device(config-if)# spanning-tree guard root
Device(config-if)#
```

The following example shows how to enable root guard on an interface using an interface template:

```
Device# configure terminal
Device(config)# template user-template1
Device(config-template)# spanning-tree guard root
Device(config-template)# end
```

Related Commands

Command	Description
show spanning-tree	Displays information about the spanning-tree state.
spanning-tree loopguard default	Enables loop guard as a default on all ports of a given bridge.

spanning-tree link-type

To configure a link type for a port, use the **spanning-tree link-type** command in the interface configuration and template configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree link-type { **point-to-point** | **shared** }
no spanning-tree link-type

Syntax Description

point-to-point	Specifies that the interface is a point-to-point link.
shared	Specifies that the interface is a shared medium.

Command Default

Link type is automatically derived from the duplex setting unless you explicitly configure the link type.

Command Modes

Interface configuration (config-if)

Template configuration (config-template)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Rapid Spanning Tree Protocol Plus (RSTP+) fast transition works only on point-to-point links between two bridges.

By default, the switch derives the link type of a port from the duplex mode. A full-duplex port is considered as a point-to-point link while a half-duplex configuration is assumed to be on a shared link.

If you designate a port as a shared link, RSTP+ fast transition is forbidden, regardless of the duplex setting.

If you connect a port (local port) to a remote port through a point-to-point link and the local port becomes a designated port, the device negotiates with the remote port and rapidly changes the local port to the forwarding state

Examples

This example shows how to configure the port as a shared link:

```
Device(config-if)# spanning-tree link-type shared
Device(config-if)#
```

The following example shows how to configure the port as a shared link using an interface template:

```
Device# configure terminal
Device(config)# template user-template1
Device(config-template)# spanning-tree link-type shared
Device(config-template)# end
```

Related Commands

Command	Description
show spanning-tree interface	Displays information about the spanning-tree state.

spanning-tree loopguard default

To enable loop guard as a default on all ports of a given bridge, use the **spanning-tree loopguard default** command in global configuration mode. To disable loop guard, use the **no** form of this command.

spanning-tree loopguard default
no spanning-tree loopguard default

Syntax Description

This command has no arguments or keywords.

Command Default

Loop guard is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Loop guard provides additional security in the bridge network. Loop guard prevents alternate or root ports from becoming the designated port due to a failure that could lead to a unidirectional link.

Loop guard operates only on ports that are considered point to point by the spanning tree.

The individual loop-guard port configuration overrides this command.

Examples

This example shows how to enable loop guard:

```
Device(config)# spanning-tree loopguard default
Device(config)#
```

Related Commands

Command	Description
show spanning-tree	Displays information about the spanning-tree state.
spanning-tree guard	Enables or disables the guard mode.

spanning-tree mode

To switch between Per-VLAN Spanning Tree+ (PVST+), Rapid-PVST+, and Multiple Spanning Tree (MST) modes, use the **spanning-tree mode** command in global configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree mode [{ **pvst** | **mst** | **rapid-pvst** }]
no spanning-tree mode

Syntax Description

pvst	(Optional) PVST+ mode.
mst	(Optional) MST mode.
rapid-pvst	(Optional) Rapid-PVST+ mode.

Command Default

pvst

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Note Be careful when using the **spanning-tree mode** command to switch between PVST+, Rapid-PVST+, and MST modes. When you enter the command, all spanning-tree instances are stopped for the previous mode and are restarted in the new mode. Using this command may cause disruption of user traffic.

Examples

This example shows how to switch to MST mode:

```
Device(config)# spanning-tree mode mst
Device(config)#
```

This example shows how to return to the default mode (PVST+):

```
Device(config)# no spanning-tree mode
Device(config)#
```

Related Commands

Command	Description
show spanning-tree mst	Displays the information about the MST protocol.

spanning-tree mst

To set the priority parameters or configure the device as a root for any Multiple Spanning Tree (MST) instance, use the **spanning-tree mst** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree mst *instance-id* { **priority** *priority* | **root** { **primary** | **secondary** } }
no spanning-tree mst *instance-id* { { **priority** *priority* | **root** { **primary** | **secondary** } } }

Syntax Description

priority *priority*	Port priority for an instance. The range is from 0 to 61440 in increments of 4096.
root	Configures the device as a root.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Examples

This example shows how to set the priority:

```
Device(config-if)#
spanning-tree mst 0 priority 1
Device(config-if)#
```

This example shows how to set the device as a primary root:

```
Device(config-if)#
spanning-tree mst 0 root primary
Device(config-if)#
```

Related Commands

Command	Description
show spanning-tree mst	Displays the information about the MST protocol.

spanning-tree mst configuration

To enter MST-configuration submode, use the **spanning-tree mst configuration** command in global configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree mst configuration
no spanning-tree mst configuration

Syntax Description

This command has no arguments or keywords.

Command Default

The default value for the Multiple Spanning Tree (MST) configuration is the default value for all its parameters:

- No VLANs are mapped to any MST instance (all VLANs are mapped to the Common and Internal Spanning Tree [CIST] instance).
- The region name is an empty string.
- The revision number is 0.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The MST configuration consists of three main parameters:

- Instance VLAN mapping: See the **instance** command.
- Region name: See the **name** command (MST configuration submode).
- Configuration revision number: See the **revision** command.

The **abort** and **exit** commands allow you to exit MST configuration submode. The difference between the two commands depends on whether you want to save your changes or not.

The **exit** command commits all the changes before leaving MST configuration submode. If you do not map secondary VLANs to the same instance as the associated primary VLAN, when you exit MST-configuration submode, a warning message displays and lists the secondary VLANs that are not mapped to the same instance as the associated primary VLAN. The warning message is as follows:

```
These secondary vlans are not mapped to the same instance as their primary:
-> 3
```

The **abort** command leaves MST-configuration submode without committing any changes.

Changing an MST-configuration submode parameter can cause connectivity loss. To reduce service disruptions, when you enter MST-configuration submode, make changes to a copy of the current MST configuration. When you are done editing the configuration, you can apply all the changes at once by using the exit keyword, or you can exit the submode without committing any change to the configuration by using the abort keyword.

In the unlikely event that two users commit a new configuration at exactly at the same time, this warning message displays:

```
% MST CFG:Configuration change lost because of concurrent access
```

Examples

This example shows how to enter MST-configuration submode:

```
Device(config)# spanning-tree mst configuration
Device(config-mst)#
```

This example shows how to reset the MST configuration to the default settings:

```
Device(config)# no spanning-tree mst configuration
Device(config)#
```

Related Commands

Command	Description
instance	Maps a VLAN or a set of VLANs to an MST instance.
name (MST)	Sets the name of an MST region.
revision	Sets the revision number for the MST configuration.
show spanning-tree mst	Displays the information about the MST protocol.

spanning-tree mst forward-time

To set the forward-delay timer for all the instances on the device, use the **spanning-tree mst forward-time** command in global configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree mst forward-time *seconds*
no spanning-tree mst forward-time

Syntax Description

seconds	Number of seconds to set the forward-delay timer for all the instances on the device. The range is from 4 to 30 seconds.

Command Default

15 seconds.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Examples

This example shows how to set the forward-delay timer:

```
Device(config)# spanning-tree mst forward-time 20
Device(config)#
```

Related Commands

Command	Description
show spanning-tree mst	Displays the information about the MST protocol.

spanning-tree mst hello-time

To set the hello-time delay timer for all the instances on the device, use the **spanning-tree mst hello-time** command in global configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree mst hello-time *seconds*
no spanning-tree mst hello-time

Syntax Description

seconds	Number of seconds to set the hello-time delay timer for all the instances on the device. The range is from 1 to 10 in seconds.

Command Default

2 seconds

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

If you do not specify the *hello-time* value, the value is calculated from the network diameter.

Examples

This example shows how to set the hello-time delay timer:

```
Device(config)# spanning-tree mst hello-time 3
Device(config)#
```

Related Commands

Command	Description
show spanning-tree mst	Displays the information about the MST protocol.

spanning-tree mst max-age

To set the max-age timer for all the instances on the device, use the **spanning-tree mst max-age** command in global configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree mst max-age *seconds*
no spanning-tree mst max-age

Syntax Description

seconds	Number of seconds to set the max-age timer for all the instances on the device. The range is from 6 to 40 in seconds.

Command Default

20 seconds

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Examples

This example shows how to set the max-age timer:

```
Device(config)# spanning-tree mst max-age 40
Device(config)#
```

Related Commands

Command	Description
show spanning-tree mst	Displays the information about the MST protocol.

spanning-tree mst max-hops

To specify the number of possible hops in the region before a bridge protocol data unit (BPDU) is discarded, use the **spanning-tree mst max-hops** command in global configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree mst max-hops *hopnumber*
no spanning-tree mst max-hops

Syntax Description

hopnumber	Number of possible hops in the region before a BPDU is discarded. The range is from 1 to 255 hops.

Command Default

20 hops

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Examples

This example shows how to set the number of possible hops:

```
Device(config)# spanning-tree mst max-hops 25
Device(config)#
```

Related Commands

Command	Description
show spanning-tree mst	Displays the information about the MST protocol.

spanning-tree mst pre-standard

To configure a port to transmit only prestandard bridge protocol data units (BPDUs), use the **spanning-tree mst pre-standard** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree mst pre-standard
no spanning-tree mst pre-standard

Syntax Description

This command has no arguments or keywords.

Command Default

The default is to automatically detect prestandard neighbors.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Even with the default configuration, the port can receive both prestandard and standard BPDUs.

Prestandard BPDUs are based on the Cisco IOS Multiple Spanning Tree (MST) implementation that was created before the IEEE standard was finalized. Standard BPDUs are based on the finalized IEEE standard.

If you configure a port to transmit prestandard BPDUs only, the prestandard flag displays in the **show spanning-tree** commands. The variations of the prestandard flag are as follows:

- Pre-STD (or pre-standard in long format): This flag displays if the port is configured to transmit prestandard BPDUs and if a prestandard neighbor bridge has been detected on this interface.
- Pre-STD-Cf (or pre-standard (config) in long format): This flag displays if the port is configured to transmit prestandard BPDUs but a prestandard BPDU has not been received on the port, the autodetection mechanism has failed, or a misconfiguration, if there is no prestandard neighbor, has occurred.
- Pre-STD-Rx (or pre-standard (rcvd) in long format): This flag displays when a prestandard BPDU has been received on the port but it has not been configured to send prestandard BPDUs. The port will send prestandard BPDUs, but we recommend that you change the port configuration so that the interaction with the prestandard neighbor does not rely only on the autodetection mechanism.

If the MST configuration is not compatible with the prestandard (if it includes an instance ID greater than 15), only standard MST BPDUs are transmitted, regardless of the STP configuration on the port.

Examples

This example shows how to configure a port to transmit only prestandard BPDUs:

```
Router(config-if)# spanning-tree mst pre-standard
Router(config-if)#
```

Related Commands

Command	Description
show spanning-tree mst	Displays the information about the MST protocol.

spanning-tree mst priority

To set the bridge priority for an instance, use the **spanning-tree mst priority** command in global configuration mode. To return to the default setting, use the **no** form of this command.

spanning-tree mst *instance* **priority** *priority*
no spanning-tree mst priority

Syntax Description

instance	Instance identification number; valid values are from 0 to 4094.
priority *priority*	Specifies the bridge priority; see the "Usage Guidelines" section for valid values and additional information.

Command Default

priority is **32768**

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

You can set the bridge priority in increments of 4096 only. When you set the priority, valid values are **0**, **4096**, **8192**, **12288**, **16384**, **20480**, **24576**, **28672**, **32768**, **36864**, **40960**, **45056**, **49152**, **53248**, **57344**, and **61440**.

You can set the *priority* to **0** to make the switch root.

You can enter *instance* as a single instance or a range of instances, for example, 0-3,5,7-9.

Examples

This example shows how to set the bridge priority:

```
Device(config)# spanning-tree mst 0 priority 4096
Device(config)#
```

Related Commands

Command	Description
show spanning-tree mst	Displays the information about the MST protocol.

spanning-tree mst root

To designate the primary and secondary root switch and set the timer value for an instance, use the **spanning-tree mst root** command in global configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree mst *instance* **root** { **primary** | **secondary** } [**diameter** *diameter* [**hello-time** *seconds*]]
no spanning-tree mst *instance* **root**

Syntax Description

instance	Instance identification number. The range is from 0 to 4094.
primary	Specifies the high enough priority (low value) to make the root of the spanning-tree instance.
secondary	Specifies the switch as a secondary root, should the primary root fail.
diameter *diameter*	(Optional) Specifies the timer values for the root switch that are based on the network diameter. The range is from 1 to 7.
hello-time *seconds*	(Optional) Specifies the duration between the generation of configuration messages by the root switch.

Command Default

The **spanning-tree mst root** command has no default settings.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

You can enter *instance* as a single instance or a range of instances, for example, 0-3,5,7-9.

The **spanning-tree mst root secondary** value is 16384.

The **diameter** *diameter* and **hello-time** *seconds* keywords and arguments are available for instance 0 only.

If you do not specify the *seconds* argument, the value for it is calculated from the network diameter.

Examples

This example shows how to designate the primary root switch and timer values for an instance:

```
Router(config)# spanning-tree mst 0 root primary diameter 7 hello-time 2
Router(config)# spanning-tree mst 5 root primary
Router(config)#
```

Related Commands

Command	Description
show spanning-tree mst	Displays the information about the MST protocol.

spanning-tree mst simulate pvst global

To enable Per-VLAN Spanning Tree (PVST) simulation globally, enter the **spanning-tree mst simulate pvst global** command in global configuration mode. To disable PVST simulation globally, enter the **no** form of this command.

spanning-tree mst simulate pvst global
no spanning-tree mst simulate pvst global

Syntax Description

This command has no arguments or keywords.

Command Default

PVST simulation is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	Support for this command was introduced.

Usage Guidelines

PVST simulation is enabled by default so that all interfaces on the device interoperate between Multiple Spanning Tree (MST) and Rapid Per-VLAN Spanning Tree Plus (PVST+). To prevent an accidental connection to a device that does not run MST as the default Spanning Tree Protocol (STP) mode, you can disable PVST simulation. If you disable PVST simulation, the MST-enabled port moves to the blocking state once it detects it is connected to a Rapid PVST+-enabled port. This port remains in the inconsistent state until the port stops receiving Bridge Protocol Data Units (BPDUs), and then the port resumes the normal STP transition process.

To override the global PVST simulation setting for a port, enter the **spanning-tree mst simulate pvst** interface command in the interface command mode.

Examples

This example shows how to prevent the switch from automatically interoperating with a connecting device that is running Rapid PVST+:

```
Device(config)#
no spanning-tree mst simulate pvst global
Device(config)#
```

Related Commands

Command	Description
show spanning-tree mst	Displays the information about the MST protocol.

spanning-tree pathcost method

To set the default path-cost calculation method, use the **spanning-tree pathcost method** command in global configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree pathcost method { **long** | **short** }
no spanning-tree pathcost method

Syntax Description

long	Specifies the 32-bit based values for default port-path costs.
short	Specifies the 16-bit based values for default port-path costs.

Command Default

short

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The **long** path-cost calculation method utilizes all 32 bits for path-cost calculation and yields values in the range of 1 through 200,000,000.

The **short** path-cost calculation method (16 bits) yields values in the range of 1 through 65535.

Examples

This example shows how to set the default path-cost calculation method to long:

```
Device(config
#) spanning-tree pathcost method long
Device(config
#)
```

This example shows how to set the default path-cost calculation method to short:

```
Device(config
#) spanning-tree pathcost method short
Device(config
#)
```

Related Commands

Command	Description
show spanning-tree	Displays information about the spanning-tree state.

spanning-tree port-priority

To set an interface priority when two bridges tie for position as the root bridge, use the **spanning-tree port-priority** command in interface configuration and template configuration mode. To revert to the default value, use the **no** form of this command.

spanning-tree port-priority *port-priority*
no spanning-tree port-priority

Syntax Description

port-priority	Port priority. The range is from 0 to 240 in increments of 16 . The default is 128.

Command Default

The default port priority is 128.

Command Modes

Interface configuration (config-if)

Template configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The priority you set breaks the tie between two bridges to be designated as a root bridge.

Examples

The following example shows how to increase the likelihood that spanning-tree instance 20 is chosen as the root-bridge on interface Ethernet 2/0:

```
Device(config)# interface ethernet 2/0
Device(config-if)# spanning-tree port-priority 20
Device(config-if)#
```

The following example shows how increase the likelihood that spanning-tree instance 20 is chosen as the root-bridge on an interface using an interface template:

```
Device# configure terminal
Device(config)# template user-template1
Device(config-template)# spanning-tree port-priority 20
Device(config-template)# end
```

Related Commands

Command	Description
show spanning-tree	Displays spanning-tree information for the specified spanning-tree instances.
spanning-tree cost	Sets the path cost of the interface for STP calculations.
spanning-tree portfast (global)	Enables PortFast mode, where the interface is immediately put into the forwarding state upon linkup without waiting for the timer to expire.

Command	Description
spanning-tree uplinkfast	Enables the UplinkFast feature.
spanning-tree vlan	Configures STP on a per-VLAN basis.

spanning-tree portfast edge bpdufilter default

To enable bridge protocol data unit (BPDU) filtering by default on all PortFast ports, use the **spanning-tree portfast edge bpdufilter default** command in global configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree portfast edge bpdufilter default
no spanning-tree portfast edge bpdufilter default

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The **spanning-tree portfast edge bpdufilter** command enables BPDU filtering globally on PortFast ports. BPDU filtering prevents a port from sending or receiving any BPDUs.

You can override the effects of the **portfast edge bpdufilter default** command by configuring BPDU filtering at the interface level.

Note Be careful when enabling BPDU filtering. The feature's functionality is different when you enable it on a per-port basis or globally. When enabled globally, BPDU filtering is applied only on ports that are in an operational PortFast state. Ports send a few BPDUs at linkup before they effectively filter outbound BPDUs. If a BPDU is received on an edge port, it immediately loses its operational PortFast status and BPDU filtering is disabled. When enabled locally on a port, BPDU filtering prevents the device from receiving or sending BPDUs on this port.

Caution Be careful when using this command. Using this command incorrectly can cause bridging loops.

Examples

This example shows how to enable BPDU filtering by default:

```
Device(config)#
spanning-tree portfast edge bpdufilter default
Device(config)#
```

Related Commands

Command	Description
show spanning-tree mst	Displays the information about the MST protocol.

Command	Description
spanning-tree bpdufilter	Enables BPDU filtering on the interface.

spanning-tree portfast edge bpduguard default

To enable bridge protocol data unit (BPDU) guard by default on all PortFast ports, use the **spanning-tree portfast edge bpduguard default** command in global configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree portfast edge bpduguard default
no spanning-tree portfast edge bpduguard default

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

⚠

Caution Be careful when using this command. You should use this command only with interfaces that connect to end stations; otherwise, an accidental topology loop could cause a data-packet loop and disrupt the device and network operation.

BPDU guard disables a port if it receives a BPDU. BPDU guard is applied only on ports that are PortFast enabled and are in an operational PortFast state.

Examples

This example shows how to enable BPDU guard by default:

```
Device(config)#
spanning-tree portfast edge bpduguard default
Device(config)#
```

Related Commands

Command	Description
show spanning-tree mst	Displays the information about the MST protocol.
spanning-tree bpdufilter	Enables BPDU filtering on the interface.

spanning-tree portfast default

To enable PortFast by default on all access ports, use the **spanning-tree portfast** {**edge** | **network** | **normal**} **default** command in global configuration mode. To disable PortFast by default on all access ports, use the **no** form of this command.

spanning-tree portfast { **edge** [{ **bpdufilter** | **bpduguard** }] | **network** | **normal** } **default**
no spanning-tree portfast { **edge** [{ **bpdufilter** | **bpduguard** }] | **network** | **normal** } **default**

Syntax Description

bpdufilter	Enables PortFast edge BPDU filter by default on all PortFast edge ports.
bpduguard	Enables PortFast edge BPDU guard by default on all PortFast edge ports.
edge	Enables PortFast edge mode by default on all switch access ports.
network	Enables PortFast network mode by default on all switch access ports.
normal	Enables PortFast normal mode by default on all switch access ports.

Command Default

PortFast is disabled by default on all access ports.

Command Modes

Global configuration (config)

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Note Be careful when using this command. You should use this command only with interfaces that connect to end stations; otherwise, an accidental topology loop could cause a data-packet loop and disrupt the operation of the router or switch and the network.

An interface with PortFast mode enabled is moved directly to the spanning-tree forwarding state when linkup occurs without waiting for the standard forward-time delay.

You can enable PortFast mode on individual interfaces using the **spanning-tree portfast** (interface) command.

Examples

This example shows how to enable PortFast edge mode with BPDU Guard by default on all access ports:

```
Device(config)#
spanning-tree portfast edge bpduguard default
Device(config)#
```

Related Commands

Command	Description
show spanning-tree	Displays information about the spanning-tree state.
spanning-tree portfast (interface)	Enables PortFast on a specific interface.

spanning-tree transmit hold-count

To specify the transmit hold count, use the **spanning-tree transmit hold-count** command in global configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree transmit hold-count *value*
no spanning-tree transmit hold-count

Syntax Description

value	Number of bridge protocol data units (BPDUs) that can be sent before pausing for 1 second. The range is from 1 to 20.

Command Default

value is **6**

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

This command is supported on all spanning-tree modes.

The transmit hold count determines the number of BPDUs that can be sent before pausing for 1 second.

Note Changing this parameter to a higher value may have a significant impact on CPU utilization, especially in rapid-Per-VLAN Spanning Tree (PVST) mode. Lowering this parameter could slow convergence in some scenarios. We recommend that you do not change the value from the default setting.

If you change the *value* setting, enter the **show running-config** command to verify the change.

If you delete the command, use the **show spanning-tree mst** command to verify the deletion.

Examples

This example shows how to specify the transmit hold count:

```
Device(config)# spanning-tree transmit hold-count 8
Device(config)#
```

Related Commands

Command	Description
show running-config	Displays the status and configuration of the module or Layer 2 VLAN.
show spanning-tree mst	Display the information about the MST protocol.

spanning-tree uplinkfast

To enable UplinkFast, use the **spanning-tree uplinkfast** command in global configuration mode. To disable UplinkFast, use the **no** form of this command.

spanning-tree uplinkfast [**max-update-rate** *packets-per-second*]
no spanning-tree uplinkfast [**max-update-rate**]

Syntax Description

max-update-rate *packets-per-second*	(Optional) Specifies the maximum rate (in packets per second) at which update packets are sent. The range is from 0 to 32000.

Command Default

The defaults are as follows:

- UplinkFast is disabled.
- *packets-per-second* is 150 packets per second.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Use the **spanning-tree uplinkfast max-update-rate** command to enable UplinkFast (if it is not already enabled) and change the rate at which update packets are sent. Use the **no** form of this command to return to the default rate.

Examples

This example shows how to enable UplinkFast and set the maximum rate to 200 packets per second:

```
Device(config)#
 spanning-tree uplinkfast max-update-rate 200
Device(config)#
```

Related Commands

Command	Description
show spanning-tree	Displays information about the spanning-tree state.

spanning-tree vlan

To configure Spanning Tree Protocol (STP) on a per-virtual LAN (VLAN) basis, use the **spanning-tree vlan** command in global configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree vlan *vlan-id* [{ **forward-time** *seconds* | **hello-time** *seconds* | **max-age** *seconds* | **priority** *priority* | **root** [{ **primary** | **secondary** }] }]
no spanning-tree vlan *vlan-id* [{ **forward-time** | **hello-time** | **max-age** | **priority** | **root** }]

Syntax Description

vlan id	VLAN identification number. The range is from 1 to 4094.
forward-time *seconds*	(Optional) Sets the STP forward delay time. The range is from 4 to 30 seconds.
hello-time *seconds*	(Optional) Specifies the duration, in seconds, between the generation of configuration messages by the root switch. The range is from 1 to 10 seconds.
max-age *seconds*	(Optional) Sets the maximum number of seconds the information in a bridge packet data unit (BPDU) is valid. the range is from 6 to 40 seconds.
priority *priority*	(Optional) Sets the STP bridge priority. the range is from 0 to 65535.
root primary	(Optional) Forces this switch to be the root bridge.
root secondary	(Optional) Specifies this switch to act as the root switch should the primary root fail.

Command Default

The defaults are:

- **forward-time**: 15 seconds
- **hello-time**: 2 seconds
- **max-age**: 20 seconds
- **priority**: The default with IEEE STP enabled is 32768; the default with STP enabled is 128.
- **root** : No STP root

When you issue the **no spanning-tree vlan** *vlan_id* command, the following parameters are reset to their defaults:

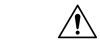
- **priority**: The default with IEEE STP enabled is 32768; the default with STP enabled is 128.
- **hello-time**: 2 seconds
- **forward-time**: 15 seconds
- **max-age**: 20 seconds

Command Modes

Global configuration (config)

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines



Caution

- When disabling spanning tree on a VLAN using the **no spanning-tree vlan** *vlan-id* command, ensure that all switches and bridges in the VLAN have spanning tree disabled. You cannot disable spanning tree on some switches and bridges in a VLAN and leave it enabled on other switches and bridges in the same VLAN because switches and bridges with spanning tree enabled have incomplete information about the physical topology of the network.
- We do not recommend disabling spanning tree, even in a topology that is free of physical loops. Spanning tree is a safeguard against misconfigurations and cabling errors. Do not disable spanning tree in a VLAN without ensuring that there are no physical loops present in the VLAN.

When you set the **max-age** *seconds* parameter, if a bridge does not hear bridge protocol data units (BPDUs) from the root bridge within the specified interval, it assumes that the network has changed and recomputes the spanning-tree topology.

The **spanning-tree root primary** command alters this switch's bridge priority to 8192. If you enter the **spanning-tree root primary** command and the switch does not become the root switch, then the bridge priority is changed to 100 less than the bridge priority of the current bridge. If the switch still does not become the root, an error results.

The **spanning-tree root secondary** command alters this switch's bridge priority to 16384. If the root switch should fail, this switch becomes the next root switch.

Use the **spanning-tree root** commands on backbone switches only.

The **spanning-tree etherchannel guard misconfig** command detects two types of errors: misconfiguration and misconnection errors. A misconfiguration error is an error between the port-channel and an individual port. A misconnection error is an error between a switch that is channeling more ports and a switch that is not using enough Spanning Tree Protocol (STP) Bridge Protocol Data Units (BPDUs) to detect the error. In this case, the switch will only error disable an EtherChannel if the switch is a nonroot switch.

Examples

The following example shows how to enable spanning tree on VLAN 200:

```
Device(config)# spanning-tree vlan 200
```

The following example shows how to configure the switch as the root switch for VLAN 10 with a network diameter of 4:

```
Device(config)# spanning-tree vlan 10 root primary diameter 4
```

The following example shows how to configure the switch as the secondary root switch for VLAN 10 with a network diameter of 4:

```
Device(config)# spanning-tree vlan 10 root secondary diameter 4
```

Related Commands

Command	Description
spanning-tree cost	Sets the path cost of the interface for STP calculations.
spanning-tree etherchannel guard misconfig	Displays an error message when a loop due to a channel misconfiguration is detected
spanning-tree port-priority	Sets an interface priority when two bridges tie for position as the root bridge.
spanning-tree uplinkfast	Enables the UplinkFast feature.
show spanning-tree	Displays spanning-tree information for the specified spanning-tree instances.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Use the **no switchport** command (without parameters) to set the interface to the routed-interface status and to erase all Layer 2 configurations. You must use this command before assigning an IP address to a routed port.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The port must be in access mode before the **switchport access vlan** command can take effect.

If the switchport mode is set to **access vlan** *vlan-id*, the port operates as a member of the specified VLAN. An access port can be assigned to only one VLAN.

The **no switchport access** command resets the access mode VLAN to the appropriate default VLAN for the device.

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**}
noswitchport mode {**access** | **dynamic** | {**auto** | **desirable**} | **trunk**}

Syntax Description

access	Sets the port to access mode (either static-access or dynamic-access depending on the setting of the **switchport access vlan** interface configuration command). The port is set to access unconditionally and operates as a nontrunking, single VLAN interface that sends and receives nonencapsulated (non-tagged) frames. An access port can be assigned to only one VLAN.
dynamic auto	Sets the port trunking mode dynamic parameter to auto to specify that the interface convert the link to a trunk link. This is the default switchport mode.
dynamic desirable	Sets the port trunking mode dynamic parameter to desirable to specify that the interface actively attempt to convert the link to a trunk link.
trunk	Sets the port to trunk unconditionally. The port is a trunking VLAN Layer 2 interface. The port sends and receives encapsulated (tagged) frames that identify the VLAN of origination. A trunk is a point-to-point link between two switches or between a switch and a router.

Command Default

The default mode is **dynamic auto**.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

A configuration that uses the **access**,or **trunk** keywords takes effect only when you configure the port in the appropriate mode by using the **switchport mode** command. The static-access and trunk configuration are saved, but only one configuration is active at a time.

When you enter **access** mode, the interface changes to permanent nontrunking mode and negotiates to convert the link into a nontrunk link even if the neighboring interface does not agree to the change.

When you enter **trunk** mode, the interface changes to permanent trunking mode and negotiates to convert the link into a trunk link even if the interface connecting to it does not agree to the change.

When you enter **dynamic auto** mode, the interface converts the link to a trunk link if the neighboring interface is set to **trunk** or **desirable** mode.

When you enter **dynamic desirable** mode, the interface becomes a trunk interface if the neighboring interface is set to **trunk**, **desirable**, or **auto** mode.

To autonegotiate trunking, the interfaces must be in the same VLAN Trunking Protocol (VTP) domain. Trunk negotiation is managed by the Dynamic Trunking Protocol (DTP), which is a point-to-point protocol. However, some internetworking devices might forward DTP frames improperly, which could cause misconfigurations. To avoid this problem, configure interfaces connected to devices that do not support DTP to not forward DTP frames, which turns off DTP.

- If you do not intend to trunk across those links, use the **switchport mode access** 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 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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The **no switchport nonegotiate** command removes nonegotiate status.

This command is valid only when the interface switchport mode is access or trunk (configured by using the **switchport mode access** or the **switchport mode trunk** interface configuration command). This command returns an error if you attempt to execute it in dynamic (auto or desirable) mode.

Internetworking devices that do not support DTP might forward DTP frames improperly and cause misconfigurations. To avoid this problem, turn off DTP by using the **switchport nonegotiate** command to configure the interfaces connected to devices that do not support DTP to not forward DTP frames.

When you enter the **switchport nonegotiate** command, DTP negotiation packets are not sent on the interface. The device does or does not trunk according to the **mode** parameter: **access** or **trunk.**

- If you do not intend to trunk across those links, use the **switchport mode access** interface configuration command to disable trunking.
- To enable trunking on a device that does not support DTP, use the **switchport mode trunk** and **switchport nonegotiate** interface configuration commands to cause the interface to become a trunk but to not generate DTP frames.

This example shows how to cause a port to refrain from negotiating trunking mode and to act as a trunk or access port (depending on the mode set):

```
Device> 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 voice vlan

To configure voice VLAN on the port, use the **switchport voice vlan** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

switchport voice vlan {*vlan-id* | **dot1p** | **none** | **untagged** | **name** *vlan_name*}
no switchport voice vlan

Syntax Description

vlan-id	The VLAN to be used for voice traffic. The range is 1 to 4094. By default, the IP phone forwards the voice traffic with an IEEE 802.1Q priority of 5.
dot1p	Configures the telephone to use IEEE 802.1p priority tagging and uses VLAN 0 (the native VLAN). By default, the Cisco IP phone forwards the voice traffic with an IEEE 802.1p priority of 5.
none	Does not instruct the IP telephone about the voice VLAN. The telephone uses the configuration from the telephone key pad.
untagged	Configures the telephone to send untagged voice traffic. This is the default for the telephone.
name *vlan_name*	(Optional) Specifies the VLAN name to be used for voice traffic. You can enter up to 128 characters.

Command Default

The default is not to automatically configure the telephone (**none**).

The telephone default is not to tag frames.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
Device> enable
Device# configure terminal
Device(config)# vlan 55
Device(config-vlan)# name test
Device(config-vlan)# end
```

Part 2 - Checking the VLAN database:

```
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:

```
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:

```
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:

```
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** | **message time** *message-timer-interval*}
no udld {**aggressive** | **enable** | **message**}

Syntax Description

aggressive	Enables UDLD in aggressive mode on all fiber-optic interfaces.
enable	Enables UDLD in normal mode on all fiber-optic interfaces.
message time *message-timer-interval*	Configures the period of time between UDLD probe messages on ports that are in the advertisement phase and are determined to be bidirectional. The range is 1 to 90 seconds. The default is 15 seconds.

Command Default

UDLD is disabled on all interfaces.

The message timer is set at 15 seconds.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

UDLD supports two modes of operation: normal (the default) and aggressive. In normal mode, UDLD detects unidirectional links due to misconnected interfaces on fiber-optic connections. In aggressive mode, UDLD also detects unidirectional links due to one-way traffic on fiber-optic and twisted-pair links and due to misconnected interfaces on fiber-optic links.

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 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. To return to the **udld** command setting in global configuration mode or to disable UDLD if entered for a nonfiber-optic port, use the **no** form of this command.

udld port [**aggressive**]
no udld port [**aggressive**]

Syntax Description

aggressive	(Optional) Enables UDLD in aggressive mode on the specified interface.

Command Default

On fiber-optic interfaces, UDLD is disabled and fiber-optic interfaces enable UDLD according to the state of the **udld enable** or **udld aggressive** command global configuration mode.

On nonfiber-optic interfaces, UDLD is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

A UDLD-capable port cannot detect a unidirectional link if it is connected to a UDLD-incapable port of another device.

UDLD supports two modes of operation: normal (the default) and aggressive. In normal mode, UDLD detects unidirectional links due to misconnected interfaces on fiber-optic connections. In aggressive mode, UDLD also detects unidirectional links due to one-way traffic on fiber-optic and twisted-pair links and due to misconnected interfaces on fiber-optic links.

To enable UDLD in normal mode, use the **udld port** command in interface configuration mode. To enable UDLD in aggressive mode, use the **udld port aggressive** command in interface configuration mode.

Use the **no udld port** command on fiber-optic ports to return control of UDLD to the **udld enable** global configuration command or to disable UDLD on nonfiber-optic ports.

Use the **udld port aggressive** command on fiber-optic ports to override the setting of the **udld enable** or **udld aggressive** command in global configuration mode. Use the **no** form 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 **no udld port** 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* commands in global configuration mode automatically recover from the UDLD error-disabled state.

This example shows how to enable UDLD on an 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** command in global configuration mode:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet6/0/1
Device(config-if)# no udld port
```

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

udld reset

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

If the interface configuration is still enabled for UDLD, these ports begin to run UDLD again and are disabled for the same reason if the problem has not been corrected.

This example shows how to reset all interfaces disabled by UDLD:

```
Device> enable
Device# udld reset
1 ports shutdown by UDLD were reset.
```

vlan dot1q tag native

To enable tagging of native VLAN frames on all IEEE 802.1Q trunk ports, use the **vlan dot1q tag native** command in global configuration mode. To return to the default setting, use the **no** form of this command.

vlan dot1q tag native
no vlan dot1q tag native

Syntax Description

This command has no arguments or keywords.

Command Default

The IEEE 802.1Q native VLAN tagging is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

When enabled, native VLAN packets going out of all IEEE 802.1Q trunk ports are tagged.

When disabled, native VLAN packets going out of all IEEE 802.1Q trunk ports are not tagged.

You can use this command with the IEEE 802.1Q tunneling feature. This feature operates on an edge device of a service-provider network and expands VLAN space by using a VLAN-in-VLAN hierarchy and tagging the tagged packets. You must use IEEE 802.1Q trunk ports for sending packets to the service-provider network. However, packets going through the core of the service-provider network might also be carried on IEEE 802.1Q trunks. If the native VLANs of an IEEE 802.1Q trunks match the native VLAN of a tunneling port on the same device, traffic on the native VLAN is not tagged on the sending trunk port. This command ensures that native VLAN packets on all IEEE 802.1Q trunk ports are tagged.

For more information about IEEE 802.1Q tunneling, see the software configuration guide for this release.

This example shows how to enable IEEE 802.1Q tagging on native VLAN frames:

```
Device> enable
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.

PART VII

Network Management

- Network Management Commands, on page 825
- Flexible NetFlow Commands, on page 905

Network Management Commands

- event manager applet, on page 827
- ip wccp, on page 830
- map platform-type, on page 832
- match platform-type, on page 833
- monitor capture (interface/control plane), on page 834
- monitor capture buffer, on page 836
- monitor capture export, on page 837
- monitor capture limit, on page 838
- monitor capture start, on page 839
- monitor capture stop, on page 840
- monitor session destination, on page 841
- monitor session filter, on page 845
- monitor session source, on page 847
- show class-map type control subscriber, on page 849
- show ip sla statistics, on page 850
- show monitor, on page 852
- show monitor capture, on page 854
- show parameter-map type subscriber attribute-to-service, on page 856
- show platform software fed switch ip wccp, on page 857
- show platform software swspan , on page 859
- snmp ifmib ifindex persist, on page 861
- snmp-server enable traps, on page 862
- snmp-server enable traps bridge, on page 865
- snmp-server enable traps bulkstat, on page 866
- snmp-server enable traps call-home, on page 867
- snmp-server enable traps cef, on page 868
- snmp-server enable traps cpu, on page 869
- snmp-server enable traps envmon, on page 870
- snmp-server enable traps errdisable, on page 871
- snmp-server enable traps flash, on page 872
- snmp-server enable traps isis, on page 873
- snmp-server enable traps license, on page 874
- snmp-server enable traps mac-notification, on page 875

- snmp-server enable traps ospf, on page 876
- snmp-server enable traps pim, on page 877
- snmp-server enable traps port-security, on page 878
- snmp-server enable traps power-ethernet, on page 879
- snmp-server enable traps snmp, on page 880
- snmp-server enable traps storm-control, on page 881
- snmp-server enable traps stpx, on page 882
- snmp-server enable traps transceiver, on page 883
- snmp-server enable traps vrfmib, on page 884
- snmp-server enable traps vstack, on page 885
- snmp-server engineID, on page 886
- snmp-server group, on page 887
- snmp-server host, on page 891
- snmp-server user, on page 896
- snmp-server view, on page 900
- switchport mode access, on page 902
- switchport voice vlan, on page 903

event manager applet

To register an applet with the Embedded Event Manager (EEM) and to enter applet configuration mode, use the **event manager applet** command in global configuration mode. To unregister the applet, use the **no** form of this command.

event manager applet *applet-name* [**authorization bypass**] [**class** *class-options*] [**trap**]
no event manager applet *applet-name* [**authorization bypass**] [**class** *class-options*] [**trap**]

Syntax Description

applet-name	Name of the applet file.
authorization	(Optional) Specifies AAA authorization type for applet.
bypass	(Optional) Specifies EEM AAA authorization type bypass.
class	(Optional) Specifies the EEM policy class.
class-options	(Optional) The EEM policy class. You can specify either one of the following: • *class-letter*-- Letter from A to Z that identifies each policy class. You can specify any one *class-letter*. • **default** --Specifies the policies registered with the default class.
trap	(Optional) Generates a Simple Network Management Protocol (SNMP) trap when the policy is triggered.

Command Default

No EEM applets are registered.

Command Modes

Global configuration (config)

Command History

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

An EEM applet is a concise method for defining event screening criteria and the actions to be taken when that event occurs.

Only one event configuration command is allowed within an applet configuration. When applet configuration submode is exited and no event command is present, a warning is displayed stating that no event is associated with this applet. If no event is specified, this applet is not considered registered and the applet is not displayed. When no action is associated with this applet, events are still triggered but no actions are performed. Multiple action applet configuration commands are allowed within an applet configuration. Use the **show event manager policy registered** command to display a list of registered applets.

Before modifying an EEM applet, use the **no** form of this command to unregister the applet because the existing applet is not replaced until you exit applet configuration mode. While you are in applet configuration mode modifying the applet, the existing applet may be executing. When you exit applet configuration mode, the old applet is unregistered and the new version is registered.

Note Do not attempt making any partial modification. EEM does not support partial changes to already registered policies. EEM policy has to be always unregistered before registering again with changes.

Action configuration commands are uniquely identified using the *label* argument, which can be any string value. Actions are sorted in ascending alphanumeric key sequence using the *label* argument as the sort key and are run using this sequence.

The EEM schedules and runs policies on the basis of an event specification that is contained within the policy itself. When applet configuration mode is exited, EEM examines the event and action commands that are entered and registers the applet to be run when a specified event occurs.

The EEM policies will be assigned a class when **class** *class-letter* is specified when they are registered. EEM policies registered without a class will be assigned to the **default** class. Threads that have **default** as the class will service the default class when the thread is available for work. Threads that are assigned specific class letters will service any policy with a matching class letter when the thread is available for work.

If there is no EEM execution thread available to run the policy in the specified class and a scheduler rule for the class is configured, the policy will wait until a thread of that class is available for execution. Synchronous policies that are triggered from the same input event should be scheduled in the same execution thread. Policies will be queued in a separate queue for each class using the queue_priority as the queuing order.

When a policy is triggered and if AAA is configured it will contact the AAA server for authorization. Using the **authorization bypass** keyword combination, you can skip to contact the AAA server and run the policy immediately. EEM stores AAA bypassed policy names in a list. This list is checked when policies are triggered. If a match is found, AAA authorization is bypassed.

To avoid authorization for commands configured through the EEM policy, EEM will use named method lists, which AAA provides. These named method lists can be configured to have no command authorization.

The following is a sample AAA configuration.

This configuration assumes a TACACS+ server at 192.168.10.1 port 10000. If the TACACS+ server is not enabled, configuration commands are permitted on the console; however, EEM policy and applet CLI interactions will fail.

```
enable password lab
aaa new-model
tacacs-server host 128.107.164.152 port 10000
tacacs-server key cisco
aaa authentication login consoleline none
aaa authorization exec consoleline none
aaa authorization commands 1 consoleline none
aaa authorization commands 15 consoleline none
line con 0
 exec-timeout 0 0
 login authentication consoleline
aaa authentication login default group tacacs+ enable
aaa authorization exec default group tacacs+
aaa authorization commands 1 default group tacacs+
aaa authorization commands 15 default group tacacs+
```

The **authorization**, **class** and **trap** keywords can be used in any combination.

Examples

The following example shows an EEM applet called IPSLAping1 being registered to run when there is an exact match on the value of a specified SNMP object ID that represents a successful IP SLA

ICMP echo operation (this is equivalent to a **ping** command). Four actions are triggered when the echo operation fails, and event monitoring is disabled until after the second failure. A message that the ICMP echo operation to a server failed is sent to syslog, an SNMP trap is generated, EEM publishes an application-specific event, and a counter called IPSLA1F is incremented by a value of one.

```
Router(config)# event manager applet IPSLAping1
Router(config-applet)# event snmp oid 1.3.6.1.4.1.9.9.42.1.2.9.1.6.4 get-type exact
entry-op eq entry-val 1 exit-op eq exit-val 2 poll-interval 5
Router(config-applet)# action 1.0 syslog priority critical msg "Server IP echo failed:
OID=$_snmp_oid_val"
Router(config-applet)# action 1.1 snmp-trap strdata "EEM detected server reachability
failure to 10.1.88.9"
Router(config-applet)# action 1.2 publish-event sub-system 88000101 type 1 arg1 10.1.88.9
arg2 IPSLAEcho arg3 fail
Router(config-applet)# action 1.3 counter name _IPSLA1F value 1 op inc
```

The following example shows how to register an applet with the name one and class A and enter applet configuration mode where the timer event detector is set to trigger an event every 10 seconds. When the event is triggered, the **action syslog** command writes the message “hello world” to syslog.

```
Router(config)# event manager applet one class A
Router(config-applet)# event timer watchdog time 10
Router(config-applet)# action syslog syslog msg "hello world"
Router(config-applet)# exit
```

The following example shows how to bypass the AAA authorization when registering an applet with the name one and class A.

```
Router(config)# event manager applet one class A authorization bypass
Router(config-applet)#
```

Related Commands

Command	Description
show event manager policy registered	Displays registered EEM policies.

ip wccp

To enable the web cache service, and specify the service number that corresponds to a dynamic service that is defined by the application engine, use the **ip wccp** global configuration command on the device. Use the **no** form of this command to disable the service.

ip wccp {**web-cache** | *service-number*} [**group-address** *groupaddress*] [**group-list** *access-list*] [**redirect-list** *access-list*] [**password** *encryption-number password*]
no ip wccp {**web-cache** | *service-number*} [**group-address** *groupaddress*] [**group-list** *access-list*] [**redirect-list** *access-list*] [**password** *encryption-number password*]

Syntax Description

web-cache	Specifies the web-cache service (WCCP Version 1 and Version 2).
service-number	Dynamic service identifier, which means the service definition is dictated by the cache. The dynamic service number can be from 0 to 254. The maximum number of services is 256, which includes the web-cache service specified with the **web-cache** keyword.
group-address *groupaddress*	(Optional) Specifies the multicast group address used by the device and the application engines to participate in the service group.
group-list *access-list*	(Optional) If a multicast group address is not used, specifies a list of valid IP addresses that correspond to the application engines that are participating in the service group.
redirect-list *access-list*	(Optional) Specifies the redirect service for specific hosts or specific packets from hosts.
password *encryption-number password*	(Optional) Specifies an encryption number. The range is 0 to 7. Use 0 for not encrypted, and use 7 for proprietary. Also, specifies a password name up to seven characters in length. The device combines the password with the MD5 authentication value to create security for the connection between the device and the application engine. By default, no password is configured, and no authentication is performed.

Command Default

WCCP services are not enabled on the device.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

WCCP transparent caching bypasses Network Address Translation (NAT) when Cisco Express Forwarding switching is enabled. To work around this situation, configure WCCP transparent caching in the outgoing direction, enable Cisco Express Forwarding switching on the content engine interface, and specify the **ip wccp web-cache redirect out** command. Configure WCCP in the incoming direction on the inside interface by

specifying the **ip wccp redirect exclude in** command on the router interface facing the cache. This configuration prevents the redirection of any packets arriving on that interface.

You can also include a redirect list when configuring a service group. The specified redirect list will deny packets with a NAT (source) IP address and prevent redirection.

This command instructs a device to enable or disable support for the specified service number or the web-cache service name. A service number can be from 0 to 254. Once the service number or name is enabled, the router can participate in the establishment of a service group.

When the **no ip wccp** command is entered, the device terminates participation in the service group, deallocates space if none of the interfaces still have the service configured, and terminates the WCCP task if no other services are configured.

The keywords following the **web-cache** keyword and the *service-number* argument are optional and may be specified in any order, but only may be specified once.

Example

The following example configures a web cache, the interface connected to the application engine or the server, and the interface connected to the client:

```
Device(config)# ip wccp web-cache
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# no switchport
Device(config-if)# ip address 172.20.10.30 255.255.255.0
Device(config-if)# no shutdown
Device(config-if)# exit
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# no switchport
Device(config-if)#
*Dec  6 13:11:29.507: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/3, changed state to down

Device(config-if)# ip address 175.20.20.10 255.255.255.0
Device(config-if)# no shutdown
Device(config-if)# ip wccp web-cache redirect in
Device(config-if)# ip wccp web-cache group-listen
Device(config-if)# exit
```

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*}

Syntax Description

map-number	Parameter map number.
eq	Specifies that the filter type name is equal to the platform type name.
not-eq	Specifies that the filter type name is not equal to the platform type name.
regex	Specifies that the filter type name is a regular expression.
platform-type	Platform type for the parameter map attribute filter criteria.

Command Default

No default behavior or values.

Command Modes

Parameter-map filter (config-parameter-map-filter)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

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
```

Related Commands

Command	Description
parameter-map type subscriber attribute-to-service	Configures a subscriber parameter map and enters parameter-map filter configuration mode.

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	Name of the platform.

Command Default

No default behavior or values.

Command Modes

Control class-map filter (config-filter-control-classmap)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Examples

The following example shows how to set a class map filter to match a 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
```

Related Commands

Command	Description
class-map type control subscriber	Creates a control class and enters control class-map filter mode.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Once an attachment point has been associated with a capture point using this command, the only way to change its direction is to remove the attachment point using the **no** form of the command and reattach the attachment point with the new direction. An attachment point's direction cannot be overridden.

If an attachment point is removed from a capture point and only one attachment point is associated with it, the capture point is effectively deleted.

Multiple attachment points can be associated with a capture point by re-running this command with another attachment point. An example is provided below.

Packets captured in the output direction of an interface might not reflect the changes made by switch rewrite (includes TTL, VLAN tag, CoS, checksum, MAC addresses, DSCP, precedent, UP, etc.).

No specific order applies when defining a capture point; you can define capture point parameters in any order. The Wireshark CLI allows as many parameters as possible on a single line. This limits the number of commands required to define a capture point.

Neither VRFs, management ports, nor private VLANs can be used as attachment points.

Wireshark cannot capture packets on a destination SPAN port.

When a VLAN is used as a Wireshark attachment point, packets are captured in the input direction only.

Examples

To define a capture point using a physical interface as an attachment point:

```
Device# monitor capture mycap interface GigabitEthernet1/0/1 in
Device# monitor capture mycap match ipv4 any any
```

Note The second command defines the core filter for the capture point. This is required for a functioning capture point.

To define a capture point with multiple attachment points:

```
Device# monitor capture mycap interface GigabitEthernet1/0/1 in
Device# monitor capture mycap match ipv4 any any
Device# monitor capture mycap control-plane in
Device# show monitor capture mycap parameter
   monitor capture mycap interface GigabitEthernet1/0/1 in
   monitor capture mycap control-plane in
```

To remove an attachment point from a capture point defined with multiple attachment points:

```
Device# show monitor capture mycap parameter
   monitor capture mycap interface GigabitEthernet1/0/1 in
   monitor capture mycap control-plane in
Device# no monitor capture mycap control-plane
Device# show monitor capture mycap parameter
   monitor capture mycap interface GigabitEthernet1/0/1 in
```

monitor capture buffer

To configure the buffer for monitor capture (WireShark), use the **monitor capture buffer** command in privileged EXEC mode. To disable the monitor capture buffer or change the buffer back to a default linear buffer from a circular buffer, use the **no** form of this command.

monitor capture {*capture-name*} **buffer** {**circular** [**size** *buffer-size*] | **size** *buffer-size*}
no monitor capture {*capture-name*} **buffer** [**circular**]

Syntax Description

capture-name	The name of the capture whose buffer is to be configured.
circular	Specifies that the buffer is of a circular type. The circular type of buffer continues to capture data, even after the buffer is consumed, by overwriting the data captured previously.
size *buffer-size*	(Optional) Specifies the size of the buffer. The range is from 1 MB to 100 MB.

Command Default

A linear buffer is configured.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

When you first configure a WireShark capture, a circular buffer of a small size is suggested.

Example

To configure a circular buffer with a size of 1 MB:

```
Device# monitor capture mycap buffer circular size 1
```

monitor capture export

To export a monitor capture (WireShark) to a file, use the **monitor capture export** command in privileged EXEC mode.

monitor capture {*capture-name*} **export** *file-location* **:** *file-name*

Syntax Description

capture-name	The name of the capture to be exported.
file-location : *file-name*	(Optional) Specifies the location and file name of the capture storage file. Acceptable values for *file-location* : • flash—On-board flash storage • — USB drive

Command Default

The captured packets are not stored.

Command Modes

Privileged EXEC

Command History

Release	Modification
	This command was introduced.

Usage Guidelines

Use the **monitor capture export** command only when the storage destination is a capture buffer. The file may be stored either remotely or locally. Use this command either during capture or after the packet capture has stopped. The packet capture is stopped when one or more end conditions have been met or you entered the **monitor capture stop** command.

When WireShark is used on switches in a stack, packet captures can be stored only on the devices specified for *file-location* above that are connected to the active switch. Example: flash1 is connected to the active switch. flash2 is connected to the secondary switch. Only flash1 can be used to store packet captures.

Note Attempts to store packet captures on unsupported devices or devices not connected to the active switch will probably result in errors.

Example

To export the capture buffer contents to mycap.pcap on a flash drive:

monitor capture limit

To configure capture limits, use the **monitor capture limit** command in privileged EXEC mode. To remove the capture limits, use the **no** form of this command.

monitor capture {*capture-name*} **limit** {[**duration** *seconds*][**packet-length** *size*][**packets** *num*]}
no monitor capture {*capture-name*} **limit** [**duration**][**packet-length**][**packets**]

Syntax Description

capture-name	The name of the capture to be assigned capture limits.
duration *seconds*	(Optional) Specifies the duration of the capture, in seconds. The range is from 1 to 1000000.
packet-length *size*	(Optional) Specifies the packet length, in bytes. If the actual packet is longer than the specified length, only the first set of bytes whose number is denoted by the bytes argument is stored.
packets *num*	(Optional) Specifies the number of packets to be processed for capture.

Command Default

Capture limits are not configured.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Example

To configure a session limit of 60 seconds and a packet segment length of 400 bytes:

```
Device# monitor capture mycap limit duration 60 packet-len 400
```

monitor capture start

To start the capture of packet data at a traffic trace point into a buffer, use the **monitor capture start** command in privileged EXEC mode.

monitor capture {*capture-name*} **start**

Syntax Description

capture-name	The name of the capture to be started.

Command Default

The buffer content is not cleared.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Use the **monitor capture clear** command to enable the packet data capture after the capture point is defined. To stop the capture of packet data, use the **monitor capture stop** command.

Ensure that system resources such as CPU and memory are available before starting a capture.

Example

To start capturing buffer contents:

```
Device#  monitor capture mycap start
```

monitor capture stop

To stop the capture of packet data at a traffic trace point, use the **monitor capture stop** command in privileged EXEC mode.

monitor capture {*capture-name*} **stop**

Syntax Description

capture-name	The name of the capture to be stopped.

Command Default

The packet data capture is ongoing.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Use the **monitor capture stop** command to stop the capture of packet data that you started using the **monitor capture start** command. You can configure two types of capture buffers: linear and circular. When the linear buffer is full, data capture stops automatically. When the circular buffer is full, data capture starts from the beginning and the data is overwritten.

Example

To stop capturing buffer contents:

```
Device#  monitor capture mycap stop
```

monitor session destination

To start a new Switched Port Analyzer (SPAN) session or Remote SPAN (RSPAN) destination session, to enable ingress traffic on the destination port for a network security device (such as a Cisco IDS Sensor Appliance), and to add or delete interfaces or VLANs to or from an existing SPAN or RSPAN session, use the **monitor session destination** global configuration command. To remove the SPAN or RSPAN session or to remove destination interfaces from the SPAN or RSPAN session, use the **no** form of this command.

monitor session *session-number* **destination** {**interface** *interface-id* [**,** | **-**] [**encapsulation** {**replicate** | **dot1q**}] {**ingress** [**dot1q** | **untagged**] } | {**remote**} **vlan** *vlan-id*
no monitor session *session-number* **destination** {**interface** *interface-id* [**,** | **-**] [**encapsulation** {**replicate** | **dot1q**}] {**ingress** [**dot1q** | **untagged**] } | {**remote**} **vlan** *vlan-id*

Syntax Description

session-number	
interface *interface-id*	Specifies the destination or source interfa physical ports (including type, stack mem channel is also a valid interface type, and
,	(Optional) Specifies a series of interfaces from a previous range. Enter a space befo
-	(Optional) Specifies a range of interfaces
encapsulation replicate	(Optional) Specifies that the destination int If not selected, the default is to send pack These keywords are valid only for local S original VLAN ID; therefore, packets are ignored with the **no** form of the command
encapsulation dot1q	(Optional) Specifies that the destination in IEEE 802.1Q encapsulation. These keywords are valid only for local S original VLAN ID; therefore, packets are ignored with the **no** form of the command
ingress	Enables ingress traffic forwarding.
dot1q	(Optional) Accepts incoming packets with the default VLAN.
untagged	(Optional) Accepts incoming packets with default VLAN.
isl	Specifies ingress forwarding using ISL en
remote	Specifies the remote VLAN for an RSPAN 1006 to 4094. The RSPAN VLAN cannot be VLAN 1 (t for Token Ring and FDDI VLANs).

vlan *vlan-id*	Sets the default VLAN for ingress traffic whe

Command Default

No monitor sessions are configured.

If **encapsulation replicate** is not specified on a local SPAN destination port, packets are sent in native form with no encapsulation tag.

Ingress forwarding is disabled on destination ports.

You can specify **all**, **local**, **range** *session-range*, or **remote** with the **no monitor session** command to clear all SPAN and RSPAN, all local SPAN, a range, or all RSPAN sessions.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

A SPAN or RSPAN destination must be a physical port.

You can have a maximum of 64 destination ports on a switch or a switch stack.

Each session can include multiple ingress or egress source ports or VLANs, but you cannot combine source ports and source VLANs in a single session. Each session can include multiple destination ports.

When you use VLAN-based SPAN (VSPAN) to analyze network traffic in a VLAN or set of VLANs, all active ports in the source VLANs become source ports for the SPAN or RSPAN session. Trunk ports are included as source ports for VSPAN, and only packets with the monitored VLAN ID are sent to the destination port.

You can monitor traffic on a single port or VLAN or on a series or range of ports or VLANs. You select a series or range of interfaces or VLANs by using the [**,** | **-**] options.

If you specify a series of VLANs or interfaces, you must enter a space before and after the comma. If you specify a range of VLANs or interfaces, you must enter a space before and after the hyphen (**-**).

EtherChannel ports can be configured as SPAN or RSPAN destination ports. A physical port that is a member of an EtherChannel group can be used as a destination port, but it cannot participate in the EtherChannel group while it is as a SPAN destination.

A port used as a destination port cannot be a SPAN or RSPAN source, nor can a port be a destination port for more than one session at a time.

You can enable IEEE 802.1x authentication on a port that is a SPAN or RSPAN destination port; however, IEEE 802.1x authentication is disabled until the port is removed as a SPAN destination. If IEEE 802.1x authentication is not available on the port, the switch returns an error message. You can enable IEEE 802.1x authentication on a SPAN or RSPAN source port.

If ingress traffic forwarding is enabled for a network security device, the destination port forwards traffic at Layer 2.

Destination ports can be configured to function in these ways:

- When you enter **monitor session** *session_number* **destination interface** *interface-id* with no other keywords, egress encapsulation is untagged, and ingress forwarding is not enabled.

- When you enter **monitor session** *session_number* **destination interface** *interface-id* **ingress**, egress encapsulation is untagged; ingress encapsulation depends on the keywords that follow—**dot1q** or **untagged**.
- When you enter **monitor session** *session_number* **destination interface** *interface-id* **encapsulation replicate** with no other keywords, egress encapsulation replicates the source interface encapsulation; ingress forwarding is not enabled. (This applies to local SPAN only; RSPAN does not support encapsulation replication.)
- When you enter **monitor session** *session_number* **destination interface** *interface-id* **encapsulation replicate ingress**, egress encapsulation replicates the source interface encapsulation; ingress encapsulation depends on the keywords that follow—**dot1q** or **untagged**. (This applies to local SPAN only; RSPAN does not support encapsulation replication.)

You can verify your settings by entering the **show monitor** privileged EXEC command. You can display SPAN, RSPAN, FSPAN, and FRSPAN configuration on the switch by entering the **show running-config** privileged EXEC command. SPAN information appears near the end of the output.

Examples

This example shows how to create a local SPAN session 1 to monitor both sent and received traffic on source port 1 on stack member 1 to destination port 2 on stack member 2:

```
Device(config)# monitor session 1 source interface gigabitethernet1/0/1 both
Device(config)# monitor session 1 destination interface gigabitethernet1/0/2
```

This example shows how to delete a destination port from an existing local SPAN session:

```
Device(config)# no monitor session 2 destination interface gigabitethernet1/0/2
```

This example shows how to configure RSPAN source session 1 to monitor a source interface and to configure the destination RSPAN VLAN 900:

```
Device(config)# monitor session 1 source interface gigabitethernet1/0/1
Device(config)# monitor session 1 destination remote vlan 900
Device(config)# end
```

This example shows how to configure an RSPAN destination session 10 in the switch receiving the monitored traffic:

```
Device(config)# monitor session 10 source remote vlan 900
Device(config)# monitor session 10 destination interface gigabitethernet1/0/2
```

This example shows how to configure the destination port for ingress traffic on VLAN 5 by using a security device that supports IEEE 802.1Q encapsulation. Egress traffic replicates the source; ingress traffic uses IEEE 802.1Q encapsulation.

```
Device(config)# monitor session 2 destination interface gigabitethernet1/0/2 encapsulation
 dot1q ingress dot1q vlan 5
```

This example shows how to configure the destination port for ingress traffic on VLAN 5 by using a security device that does not support encapsulation. Egress traffic and ingress traffic are untagged.

```
Device(config)# monitor session 2 destination interface gigabitethernet1/0/2 ingress untagged
 vlan 5
```

monitor session filter

To start a new flow-based SPAN (FSPAN) session or flow-based RSPAN (FRSPAN) source or destination session, or to limit (filter) SPAN source traffic to specific VLANs, use the **monitor session filter** global configuration command. To remove filters from the SPAN or RSPAN session, use the **no** form of this command.

monitor session *session-number* **filter** {**vlan** *vlan-id* [**,** | **-**] }
no monitor session *session-number* **filter** {**vlan** *vlan-id* [**,** | **-**] }

Syntax Description

session-number	
vlan *vlan-id*	Specifies a list of VLANs as filters on trunk source ports t VLANs. The *vlan-id* range is 1 to 4094.
,	(Optional) Specifies a series of VLANs, or separates a ra Enter a space before and after the comma.
-	(Optional) Specifies a range of VLANs. Enter a space be

Command Default

No monitor sessions are configured.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

You can monitor traffic on a single VLAN or on a series or range of ports or VLANs. You select a series or range of VLANs by using the [**,** | **-**] options.

If you specify a series of VLANs, you must enter a space before and after the comma. If you specify a range of VLANs, you must enter a space before and after the hyphen (**-**).

VLAN filtering refers to analyzing network traffic on a selected set of VLANs on trunk source ports. By default, all VLANs are monitored on trunk source ports. You can use the **monitor session** *session_number* **filter vlan** *vlan-id* command to limit SPAN traffic on trunk source ports to only the specified VLANs.

VLAN monitoring and VLAN filtering are mutually exclusive. If a VLAN is a source, VLAN filtering cannot be enabled. If VLAN filtering is configured, a VLAN cannot become a source.

You can verify your settings by entering the **show monitor** privileged EXEC command. You can display SPAN, RSPAN, FSPAN, and FRSPAN configuration on the switch by entering the **show running-config** privileged EXEC command. SPAN information appears near the end of the output.

Examples

This example shows how to limit SPAN traffic in an existing session only to specific VLANs:

```
Switch(config)# monitor session 1 filter vlan 100 - 110
```

This example shows how to create a local SPAN session 1 to monitor both sent and received traffic on source port 1 on stack member 1 to destination port 2 on stack member 2 and to filter IPv4 traffic using access list number 122 in an FSPAN session:

```
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.

monitor session *session_number* **source** {**interface** *interface-id* [**,** | **-**] [**both** | **rx** | **tx**] | [**remote**] **vlan** *vlan-id* [**,** | **-**] [**both** | **rx** | **tx**]}
no monitor session *session_number* **source** {**interface** *interface-id* [**,** | **-**] [**both** | **rx** | **tx**] | [**remote**] **vlan** *vlan-id* [**,** | **-**] [**both** | **rx** | **tx**]}

Syntax Description

session_number	
interface *interface-id*	Specifies the source interface for a SPAN or RSPAN session. Valid interfaces are physical ports (including type, stack member, module, and port number). For source interface, port channel is also a valid interface type, and the valid range is 1 to 48.
,	(Optional) Specifies a series of interfaces or VLANs, or separates a range of interfaces or VLANs from a previous range. Enter a space before and after the comma.
-	(Optional) Specifies a range of interfaces or VLANs. Enter a space before and after the hyphen.
both | **rx** | **tx**	(Optional) Specifies the traffic direction to monitor. If you do not specify a traffic direction, the source interface sends both transmitted and received traffic.
remote	(Optional) Specifies the remote VLAN for an RSPAN source or destination session. The range is 2 to 1001 and 1006 to 4094. The RSPAN VLAN cannot be VLAN 1 (the default VLAN) or VLAN IDs 1002 to 1005 (reserved for Token Ring and FDDI VLANs).
vlan *vlan-id*	When used with only the **ingress** keyword, sets default VLAN for ingress traffic.

Command Default

No monitor sessions are configured.

On a source interface, the default is to monitor both received and transmitted traffic.

On a trunk interface used as a source port, all VLANs are monitored.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Traffic that enters or leaves source ports or source VLANs can be monitored by using SPAN or RSPAN. Traffic routed to source ports or source VLANs cannot be monitored.

A source can be a physical port, a port channel, or a VLAN.

Each session can include multiple ingress or egress source ports or VLANs, but you cannot combine source ports and source VLANs in a single session. Each session can include multiple destination ports.

When you use VLAN-based SPAN (VSPAN) to analyze network traffic in a VLAN or set of VLANs, all active ports in the source VLANs become source ports for the SPAN or RSPAN session. Trunk ports are included as source ports for VSPAN, and only packets with the monitored VLAN ID are sent to the destination port.

You can monitor traffic on a single port or VLAN or on a series or range of ports or VLANs. You select a series or range of interfaces or VLANs by using the [**,** | -] options.

If you specify a series of VLANs or interfaces, you must enter a space before and after the comma. If you specify a range of VLANs or interfaces, you must enter a space before and after the hyphen (-).

You can monitor individual ports while they participate in an EtherChannel, or you can monitor the entire EtherChannel bundle by specifying the **port-channel** number as the RSPAN source interface.

A port used as a destination port cannot be a SPAN or RSPAN source, nor can a port be a destination port for more than one session at a time.

You can enable IEEE 802.1x authentication on a SPAN or RSPAN source port.

You can verify your settings by entering the **show monitor** privileged EXEC command. You can display SPAN, RSPAN, FSPAN, and FRSPAN configuration on the switch by entering the **show running-config** privileged EXEC command. SPAN information appears near the end of the output.

Examples

This example shows how to create a local SPAN session 1 to monitor both sent and received traffic on source port 1 on stack member 1 to destination port 2 on stack member 2:

```
Switch(config)# monitor session 1 source interface gigabitethernet1/0/1 both
Switch(config)# monitor session 1 destination interface gigabitethernet1/0/2
```

This example shows how to configure RSPAN source session 1 to monitor multiple source interfaces and to configure the destination RSPAN VLAN 900.

```
Switch(config)# monitor session 1 source interface gigabitethernet1/0/1
Switch(config)# monitor session 1 source interface port-channel 2 tx
Switch(config)# monitor session 1 destination remote vlan 900
Switch(config)# end
```

show class-map type control subscriber

To display the 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

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

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

Class-map                 Action                       Exec  Hit  Miss  Comp
---------                 ------                       ----  ---  ----  ----
match-all platform        match platform-type C9xxx    0     0    0     0
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**] | **details**]

Syntax Description

operation-number	(Optional) Number of the operation for which operational status and statistics are displayed. Accepted values are from 1 to 2147483647.
details	(Optional) Specifies detailed output.
aggregated	(Optional) Specifies the IP SLA aggregated statistics.

Command Default

Displays output for all running IP SLA operations.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Use the **show ip sla statistics** to display the current state of IP SLA operations, including how much life the operation has left, whether the operation is active, and the completion time. The output also includes the monitoring data returned for the last (most recently completed) operation. This generated operation ID is displayed when you use the **show ip sla** configuration command for the base multicast operation, and as part of the summary statistics for the entire operation.

Enter the **show** command for a specific operation ID to display details for that one responder.

Examples

The following is sample output from the **show ip sla statistics** command:

```
Device# show ip sla statistics

Current Operational State
Entry Number: 3
Modification Time: *22:15:43.000 UTC Sun Feb 11 2001
Diagnostics Text:
Last Time this Entry was Reset: Never
Number of Octets in use by this Entry: 1332
Number of Operations Attempted: 2
Current Seconds Left in Life: 3511
Operational State of Entry: active
Latest Completion Time (milliseconds): 544
Latest Operation Start Time: *22:16:43.000 UTC Sun Feb 11 2001
Latest Oper Sense: ok
Latest Sense Description: 200  OK
```

```
Total RTT: 544
DNS RTT: 12
TCP Connection RTT: 28
HTTP Transaction RTT: 504
HTTP Message Size: 9707
```

show monitor

To display information about all Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) sessions, use the **show monitor** command in EXEC mode.

show monitor [**session** {*session_number* | **all** | **local** | **range** *list* | **remote**} [**detail**]]

Syntax Description

session	(Optional) Displays information about specified SPAN sessions.
session_number	
all	(Optional) Displays all SPAN sessions.
local	(Optional) Displays only local SPAN sessions.
range *list*	(Optional) Displays a range of SPAN sessions, where *list* is the range of valid sessions. The range is either a single session or a range of sessions described by two numbers, the lower one first, separated by a hyphen. Do not enter any spaces between comma-separated parameters or in hyphen-specified ranges. **Note** This keyword is available only in privileged EXEC mode.
remote	(Optional) Displays only remote SPAN sessions.
detail	(Optional) Displays detailed information about the specified sessions.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The output is the same for the **show monitor** command and the **show monitor session all** command.

Examples

This is an example of output for the **show monitor** user EXEC command:

```
Device# show monitor
Session 1
---------
Type : Local Session
Source Ports :
```

```
RX Only : Gi4/0/1
Both : Gi4/0/2-3,Gi4/0/5-6
Destination Ports : Gi4/0/20
Encapsulation : Replicate
Ingress : Disabled
Session 2
---------
Type : Remote Source Session
Source VLANs :
TX Only : 10
Both : 1-9
Dest RSPAN VLAN : 105
```

This is an example of output for the **show monitor** user EXEC command for local SPAN source session 1:

```
Device# show monitor session 1
Session 1
---------
Type : Local Session
Source Ports :
RX Only : Gi4/0/1
Both : Gi4/0/2-3,Gi4/0/5-6
Destination Ports : Gi4/0/20
Encapsulation : Replicate
Ingress : Disabled
```

This is an example of output for the **show monitor session all** user EXEC command when ingress traffic forwarding is enabled:

```
Device# show monitor session all
Session 1
---------
Type : Local Session
Source Ports :
Both : Gi4/0/2
Destination Ports : Gi4/0/3
Encapsulation : Native
Ingress : Enabled, default VLAN = 5
Ingress encap : DOT1Q
Session 2
---------
Type : Local Session
Source Ports :
Both : Gi4/0/8
Destination Ports : Gi4/012
Encapsulation : Replicate
Ingress : Enabled, default VLAN = 4
Ingress encap : Untagged
```

show monitor capture

To display monitor capture (WireShark) content, use the **show monitor capture** command in privileged EXEC mode.

show monitor capture [*capture-name* [**buffer**] | **file** *file-location* **:** *file-name*][**brief** | **detailed** | **display-filter** *display-filter-string*]

Syntax Description

capture-name	(Optional) Specifies the name of the capture to be displayed.
buffer	(Optional) Specifies that a buffer associated with the named capture is to be displayed.
file *file-location* : *file-name*	(Optional) Specifies the file location and name of the capture storage file to be displayed.
brief	(Optional) Specifies the display content in brief.
detailed	(Optional) Specifies detailed display content.
display-filter *display-filter-string*	Filters the display content according to the *display-filter-string*.

Command Default

Displays all capture content.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Example

The following is sample output from the **show monitor capture** command:

```
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 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

all	Displays statistics for all parameter maps.
name *parameter-map-name*	Displays statistics for the specified parameter map.

Command Modes

Privileged EXEC (#)

Command History

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

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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

This command is available only if your device is running the IP Services feature set.

The following example displays WCCP interfaces:

```
Device# show platform software fed switch 1 ip wccp interfaces

WCCP Interface Info

=====================

**** WCCP Interface: Port-channel13 iif_id: 000000000000007c (#SG:3),  VRF: 0 Ingress WCCP
 ****
port_handle:0x20000f9

List of Service Groups on this interface:
* Service group id:90 vrf_id:0 (ref count:24)
type: Dynamic     Open service      prot: PROT_TCP    l4_type: Dest ports     priority: 35
Promiscuous mode (no ports).
```

```
* Service group id:70 vrf_id:0 (ref count:24)
type: Dynamic     Open service      prot: PROT_TCP    l4_type: Dest ports     priority: 35
Promiscuous mode (no ports).


* Service group id:60 vrf_id:0 (ref count:24)
type: Dynamic     Open service      prot: PROT_TCP    l4_type: Dest ports     priority: 35
Promiscuous mode (no ports).



**** WCCP Interface: Port-channel14 iif_id: 000000000000007e (#SG:3),  VRF: 0 Ingress WCCP
 ****
port_handle:0x880000fa

List of Service Groups on this interface:
* Service group id:90 vrf_id:0 (ref count:24)
type: Dynamic     Open service      prot: PROT_TCP    l4_type: Dest ports     priority: 35
Promiscuous mode (no ports).


* Service group id:70 vrf_id:0 (ref count:24)
type: Dynamic     Open service      prot: PROT_TCP    l4_type: Dest ports     priority: 35
Promiscuous mode (no ports).
<output truncated>
```

show platform software swspan

To display switched port analyzer (SPAN) information, use the **show platform software swspan** command in privileged EXEC mode.

show platform software swspan {**switch**} {{{**F0** | **FP active**} **counters**} | **R0** | **RP active**} {**destination sess-id** *session-ID* | **source sess-id** *session-ID*}

Syntax Description

switch	Displays information about the switch.
F0	Displays information about the Embedded Service Processor (ESP) slot 0.
FP	Displays information about the ESP.
active	Displays information about the active instance of the ESP or the Route Processor (RP).
counters	Displays the SWSPAN message counters.
R0	Displays information about the RP slot 0.
RP	Displays information the RP.
destination sess-id *session-ID*	Displays information about the specified destination session.
source sess-id *session-ID*	Displays information about the specified source session.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced in a release prior to Cisco IOS XE Denali 16.1.1.

Usage Guidelines

If the session number does not exist or if the SPAN session is a remote destination session, the command output will display the following message "% Error: No Information Available."

Examples

The following is sample output from the **show platform software swspan FP active source** command:

```
Switch# show platform software swspan FP active source sess-id 0

Showing SPAN source detail info

Session ID : 0
Intf Type : PORT
Port dpidx : 30
PD Sess ID : 1
Session Type : Local
Direction : Ingress
Filter Enabled : No
ACL Configured : No
AOM Object id : 579
```

```
AOM Object Status : Done
Parent AOM object Id : 118
Parent AOM object Status : Done

Session ID : 9
Intf Type : PORT
Port dpidx : 8
PD Sess ID : 0
Session Type : Local
Direction : Ingress
Filter Enabled : No
ACL Configured : No
AOM Object id : 578
AOM Object Status : Done
Parent AOM object Id : 70
Parent AOM object Status : Done
```

The following is sample output from the **show platform software swspan RP active destination** command:

```
Switch# show platform software swspan RP active destination

Showing SPAN destination table summary info

Sess-id IF-type IF-id Sess-type
-------------------------------------
1 PORT 19 Remote
```

snmp 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

Command	Description
snmp ifindex clear	Clears any previously configured **snmp ifIndex** commands issued in interface configuration mode for a specific interface.
snmp ifindex persist	Enables ifIndex values that persist across reboots (ifIndex persistence) in the IF-MIB.

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** | **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** | **config** | **config-copy** | **config-ctid** | **copy-config** | **cpu** | **dot1x** | **energywise** | **entity** | **envmon** | **errdisable** | **event-manager** | **flash** | **fru-ctrl** | **license** | **mac-notification** | **port-security** | **power-ethernet** | **rep** | **snmp** | **stackwise** | **storm-control** | **stpx** | **syslog** | **transceiver** | **tty** | **vlan-membership** | **vlancreate** | **vlandelete** | **vstack** | **vtp**]

Syntax Description

auth-framework	(Optional) Enables SNMP CISCO-AUTH-FRAMEWORK-MIB traps.
sec-violation	(Optional) Enables SNMP camSecurityViolationNotif notifications.
bridge	(Optional) Enables SNMP STP Bridge MIB traps.*
call-home	(Optional) Enables SNMP CISCO-CALLHOME-MIB traps.*
config	(Optional) Enables SNMP configuration traps.
config-copy	(Optional) Enables SNMP configuration copy traps.
config-ctid	(Optional) Enables SNMP configuration CTID traps.
copy-config	(Optional) Enables SNMP copy-configuration traps.
cpu	(Optional) Enables CPU notification traps.*
dot1x	(Optional) Enables SNMP dot1x traps.*
energywise	(Optional) Enables SNMP energywise traps.*
entity	(Optional) Enables SNMP entity traps.
envmon	(Optional) Enables SNMP environmental monitor traps.*
errdisable	(Optional) Enables SNMP errdisable notification traps.*
event-manager	(Optional) Enables SNMP Embedded Event Manager traps.
flash	(Optional) Enables SNMP FLASH notification traps.*

fru-ctrl	(Optional) Generates entity field-replaceable unit (FRU) control traps. In a device stack, this trap refers to the insertion or removal of a device in the stack.
license	(Optional) Enables license traps.*
mac-notification	(Optional) Enables SNMP MAC Notification traps.*
port-security	(Optional) Enables SNMP port security traps.*
power-ethernet	(Optional) Enables SNMP power Ethernet traps.*
rep	(Optional) Enables SNMP Resilient Ethernet Protocol traps.
snmp	(Optional) Enables SNMP traps.*
stackwise	(Optional) Enables SNMP stackwise traps.*
storm-control	(Optional) Enables SNMP storm-control trap parameters.*
stpx	(Optional) Enables SNMP STPX MIB traps.*
syslog	(Optional) Enables SNMP syslog traps.
transceiver	(Optional) Enables SNMP transceiver traps.*
tty	(Optional) Sends TCP connection traps. This is enabled by default.
vlan-membership	(Optional) Enables SNMP VLAN membership traps.
vlancreate	(Optional) Enables SNMP VLAN-created traps.
vlandelete	(Optional) Enables SNMP VLAN-deleted traps.
vstack	(Optional) Enables SNMP Smart Install traps.*
vtp	(Optional) Enables VLAN Trunking Protocol (VTP) traps.

Command Default

The sending of SNMP traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The command options marked with an asterisk in the table above have subcommands. For more information on these subcommands, see the Related Commands section below.

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

When supported, use the **snmp-server enable traps** command to enable sending of traps or informs.

Note Though visible in the command-line help strings, the **fru-ctrl, insertion**, and **removal** keywords are not supported on the device. The **snmp-server enable informs** global configuration command is not supported. To enable the sending of SNMP inform notifications, use the **snmp-server enable traps** global configuration command combined with the **snmp-server host** *host-addr* **informs** global configuration command.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples

This example shows how to enable more than one type of SNMP trap:

```
Device(config)# snmp-server enable traps config
Device(config)# snmp-server enable traps vtp
```

snmp-server enable traps bridge

To generate STP bridge MIB traps, use the **snmp-server enable traps bridge** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps bridge [**newroot**] [**topologychange**]
no snmp-server enable traps bridge [**newroot**] [**topologychange**]

Syntax Description

newroot	(Optional) Enables SNMP STP bridge MIB new root traps.
topologychange	(Optional) Enables SNMP STP bridge MIB topology change traps.

Command Default

The sending of bridge SNMP traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples

This example shows how to send bridge new root traps to the NMS:

```
Device(config)# snmp-server enable traps bridge newroot
```

snmp-server enable traps bulkstat

To enable data-collection-MIB traps, use the **snmp-server enable traps bulkstat** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps bulkstat [**collection** | **transfer**]
no snmp-server enable traps bulkstat [**collection** | **transfer**]

Syntax Description

collection	(Optional) Enables data-collection-MIB collection traps.
transfer	(Optional) Enables data-collection-MIB transfer traps.

Command Default

The sending of data-collection-MIB traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples

This example shows how to generate data-collection-MIB collection traps:

```
Device(config)# snmp-server enable traps bulkstat collection
```

snmp-server enable traps call-home

To enable SNMP CISCO-CALLHOME-MIB traps, use the **snmp-server enable traps call-home** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps call-home [**message-send-fail** | **server-fail**]
no snmp-server enable traps call-home [**message-send-fail** | **server-fail**]

Syntax Description

message-send-fail	(Optional) Enables SNMP message-send-fail traps.
server-fail	(Optional) Enables SNMP server-fail traps.

Command Default

The sending of SNMP CISCO-CALLHOME-MIB traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples

This example shows how to generate SNMP message-send-fail traps:

```
Device(config)# snmp-server enable traps call-home message-send-fail
```

snmp-server enable traps cef

To enable SNMP Cisco Express Forwarding (CEF) traps, use the **snmp-server enable traps cef** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps cef [**inconsistency** | **peer-fib-state-change** | **peer-state-change** | **resource-failure**]
no snmp-server enable traps cef [**inconsistency** | **peer-fib-state-change** | **peer-state-change** | **resource-failure**]

Syntax Description

inconsistency	(Optional) Enables SNMP CEF Inconsistency traps.
peer-fib-state-change	(Optional) Enables SNMP CEF Peer FIB State change traps.
peer-state-change	(Optional) Enables SNMP CEF Peer state change traps.
resource-failure	(Optional) Enables SNMP CEF Resource Failure traps.

Command Default

The sending of SNMP CEF traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples

This example shows how to generate SNMP CEF inconsistency traps:

```
Device(config)# snmp-server enable traps cef inconsistency
```

snmp-server enable traps cpu

To enable CPU notifications, use the **snmp-server enable traps cpu** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps cpu [**threshold**]
no snmp-server enable traps cpu [**threshold**]

Syntax Description

threshold	(Optional) Enables CPU threshold notification.

Command Default

The sending of CPU notifications is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples

This example shows how to generate CPU threshold notifications:

```
Device(config)# snmp-server enable traps cpu threshold
```

snmp-server enable traps envmon

To enable SNMP environmental traps, use the **snmp-server enable traps envmon** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps envmon [**status**]
no snmp-server enable traps envmon [**status**]

Syntax Description

status	(Optional) Enables SNMP environmental status-change traps.

Command Default

The sending of environmental SNMP traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

In addition to enabling environmental status-change traps, the **snmp-server enable traps envmon status** command also enables traps for fan, power supply and temperature.

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 status-change traps:

```
Device(config)# snmp-server enable traps envmon status
```

snmp-server enable traps errdisable

To enable SNMP notifications of error-disabling, use the **snmp-server enable traps errdisable** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps errdisable [**notification-rate** *number-of-notifications*]
no snmp-server enable traps errdisable [**notification-rate** *number-of-notifications*]

Syntax Description

notification-rate *number-of-notifications*	(Optional) Specifies number of notifications per minute as the notification rate. Accepted values are from 0 to 10000.

Command Default

The sending of SNMP notifications of error-disabling is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples

This example shows how to set the number SNMP notifications of error-disabling to 2:

```
Device(config)# snmp-server enable traps errdisable notification-rate 2
```

snmp-server enable traps flash

To enable SNMP flash notifications, use the **snmp-server enable traps flash** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps flash [**insertion**] [**removal**]
no snmp-server enable traps flash [**insertion**] [**removal**]

Syntax Description

insertion	(Optional) Enables SNMP flash insertion notifications.
removal	(Optional) Enables SNMP flash removal notifications.

Command Default

The sending of SNMP flash notifications is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples

This example shows how to generate SNMP flash insertion notifications:

```
Device(config)# snmp-server enable traps flash insertion
```

snmp-server enable traps isis

To enable intermediate system-to-intermediate system (IS-IS) link-state routing protocol traps, use the **snmp-server enable traps isis** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps isis [**errors** | **state-change**]
no snmp-server enable traps isis [**errors** | **state-change**]

Syntax Description

errors	(Optional) Enables IS-IS error traps.
state-change	(Optional) Enables IS-IS state change traps.

Command Default

The sending of IS-IS traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples

This example shows how to generate IS-IS error traps:

```
Device(config)# snmp-server enable traps isis errors
```

snmp-server enable traps license

To enable license traps, use the **snmp-server enable traps license** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps license [**deploy**] [**error**] [**usage**]
no snmp-server enable traps license [**deploy**] [**error**] [**usage**]

Syntax Description

deploy	(Optional) Enables license deployment traps.
error	(Optional) Enables license error traps.
usage	(Optional) Enables license usage traps.

Command Default

The sending of license traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples

This example shows how to generate license deployment traps:

```
Device(config)# snmp-server enable traps license deploy
```

snmp-server enable traps mac-notification

To enable SNMP MAC notification traps, use the **snmp-server enable traps mac-notification** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps mac-notification [**change**] [**move**] [**threshold**]
no snmp-server enable traps mac-notification [**change**] [**move**] [**threshold**]

Syntax Description

change	(Optional) Enables SNMP MAC change traps.
move	(Optional) Enables SNMP MAC move traps.
threshold	(Optional) Enables SNMP MAC threshold traps.

Command Default

The sending of SNMP MAC notification traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples

This example shows how to generate SNMP MAC notification change traps:

```
Device(config)# snmp-server enable traps mac-notification change
```

snmp-server enable traps ospf

To enable SNMP Open Shortest Path First (OSPF) traps, use the **snmp-server enable traps ospf** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps ospf [**cisco-specific** | **errors** | **lsa** | **rate-limit** *rate-limit-time max-number-of-traps* | **retransmit** | **state-change**]
no snmp-server enable traps ospf [**cisco-specific** | **errors** | **lsa** | **rate-limit** *rate-limit-time max-number-of-traps* | **retransmit** | **state-change**]

Syntax Description

cisco-specific	(Optional) Enables Cisco-specific traps.
errors	(Optional) Enables error traps.
lsa	(Optional) Enables link-state advertisement (LSA) traps.
rate-limit	(Optional) Enables rate-limit traps.
rate-limit-time	(Optional) Specifies window of time in seconds for rate-limit traps. Accepted values are 2 to 60.
max-number-of-traps	(Optional) Specifies maximum number of rate-limit traps to be sent in window time.
retransmit	(Optional) Enables packet-retransmit traps.
state-change	(Optional) Enables state-change traps.

Command Default

The sending of OSPF SNMP traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples

This example shows how to enable LSA traps:

```
Device(config)# snmp-server enable traps ospf lsa
```

snmp-server enable traps pim

To enable SNMP Protocol-Independent Multicast (PIM) traps, use the **snmp-server enable traps pim** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps pim [**invalid-pim-message**] [**neighbor-change**] [**rp-mapping-change**]
no snmp-server enable traps pim [**invalid-pim-message**] [**neighbor-change**] [**rp-mapping-change**]

Syntax Description

invalid-pim-message	(Optional) Enables invalid PIM message traps.
neighbor-change	(Optional) Enables PIM neighbor-change traps.
rp-mapping-change	(Optional) Enables rendezvous point (RP)-mapping change traps.

Command Default

The sending of PIM SNMP traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples

This example shows how to enable invalid PIM message traps:

```
Device(config)# snmp-server enable traps pim invalid-pim-message
```

snmp-server enable traps port-security

To enable SNMP port security traps, use the **snmp-server enable traps port-security** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps port-security [**trap-rate** *value*]
no snmp-server enable traps port-security [**trap-rate** *value*]

Syntax Description

trap-rate *value*	(Optional) Sets the maximum number of port-security traps sent per second. The range is from 0 to 1000; the default is 0 (no limit imposed; a trap is sent at every occurrence).

Command Default

The sending of port security SNMP traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples

This example shows how to enable port-security traps at a rate of 200 per second:

```
Device(config)# snmp-server enable traps port-security trap-rate 200
```

snmp-server enable traps power-ethernet

To enable SNMP power-over-Ethernet (PoE) traps, use the **snmp-server enable traps power-ethernet** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps power-ethernet {**group** *number* | **police**}
no snmp-server enable traps power-ethernet {**group** *number* | **police**}

Syntax Description

group *number*	Enables inline power group-based traps for the specified group number. Accepted values are from 1 to 9.
police	Enables inline power policing traps.

Command Default

The sending of power-over-Ethernet SNMP traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples

This example shows how to enable power-over-Ethernet traps for group 1:

```
Device(config)# snmp-server enable traps poower-over-ethernet group 1
```

snmp-server enable traps snmp

To enable SNMP traps, use the **snmp-server enable traps snmp** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps snmp [**authentication**] [**coldstart**] [**linkdown**] [**linkup**] [**warmstart**]
no snmp-server enable traps snmp [**authentication**] [**coldstart**] [**linkdown**] [**linkup**] [**warmstart**]

Syntax Description

authentication	(Optional) Enables authentication traps.
coldstart	(Optional) Enables cold start traps.
linkdown	(Optional) Enables linkdown traps.
linkup	(Optional) Enables linkup traps.
warmstart	(Optional) Enables warmstart traps.

Command Default

The sending of SNMP traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples

This example shows how to enable a warmstart SNMP trap:

```
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.

snmp-server enable traps storm-control { **trap-rate** *number-of-minutes* }
no snmp-server enable traps storm-control { **trap-rate** }

Syntax Description

trap-rate *number-of-minutes*	(Optional) Specifies the SNMP storm-control trap rate in minutes. Accepted values are from 0 to 1000. The default is 0. Value 0 indicates that no limit is imposed and a trap is sent at every occurrence. When configured, **show run all** command output displays `no snmp-server enable traps storm-control`.

Command Default

The sending of SNMP storm-control trap parameters is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples

This example shows how to set the SNMP storm-control trap rate to 10 traps per minute:

```
Device(config)# snmp-server enable traps storm-control trap-rate 10
```

snmp-server enable traps stpx

To enable SNMP STPX MIB traps, use the **snmp-server enable traps stpx** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps stpx [**inconsistency**] [**loop-inconsistency**] [**root-inconsistency**]
no snmp-server enable traps stpx [**inconsistency**] [**loop-inconsistency**] [**root-inconsistency**]

Syntax Description

inconsistency	(Optional) Enables SNMP STPX MIB inconsistency update traps.
loop-inconsistency	(Optional) Enables SNMP STPX MIB loop inconsistency update traps.
root-inconsistency	(Optional) Enables SNMP STPX MIB root inconsistency update traps.

Command Default

The sending of SNMP STPX MIB traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples

This example shows how to generate SNMP STPX MIB inconsistency update traps:

```
Device(config)# snmp-server enable traps stpx inconsistency
```

snmp-server enable traps transceiver

To enable SNMP transceiver traps, use the **snmp-server enable traps transceiver** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps transceiver {**all**}
no snmp-server enable traps transceiver {**all**}

Syntax Description

all	(Optional) Enables all SNMP transceiver traps.

Command Default

The sending of SNMP transceiver traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples

This example shows how to set all SNMP transceiver traps:

```
Device(config)# snmp-server enable traps transceiver all
```

snmp-server enable traps vrfmib

To allow SNMP vrfmib traps, use the **snmp-server enable traps vrfmib** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps vrfmib [**vnet-trunk-down** | **vnet-trunk-up** | **vrf-down** | **vrf-up**]
no snmp-server enable traps vrfmib [**vnet-trunk-down** | **vnet-trunk-up** | **vrf-down** | **vrf-up**]

Syntax Description

vnet-trunk-down	(Optional) Enables vrfmib trunk down traps.
vnet-trunk-up	(Optional) Enables vrfmib trunk up traps.
vrf-down	(Optional) Enables vrfmib vrf down traps.
vrf-up	(Optional) Enables vrfmib vrf up traps.

Command Default

The sending of SNMP vrfmib traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples

This example shows how to generate vrfmib trunk down traps:

```
Device(config)# snmp-server enable traps vrfmib vnet-trunk-down
```

snmp-server enable traps vstack

To enable SNMP smart install traps, use the **snmp-server enable traps vstack** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps vstack [**addition**] [**failure**] [**lost**] [**operation**]
no snmp-server enable traps vstack [**addition**] [**failure**] [**lost**] [**operation**]

Syntax Description

addition	(Optional) Enables client added traps.
failure	(Optional) Enables file upload and download failure traps.
lost	(Optional) Enables client lost trap.
operation	(Optional) Enables operation mode change traps.

Command Default

The sending of SNMP smart install traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples

This example shows how to generate SNMP 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 Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

None

Examples

The following example configures a local engine ID of 123400000000000000000000:

```
Device(config)# snmp-server engineID local 1234
```

snmp-server 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-numberacl-name*}]]
no snmp-server group *group-name* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**context** *context-name*]

Syntax Description

group-name	Name of the group.
v1	Specifies that the group is using the SNMPv1 security model. SNMPv1 is the least secure of the possible SNMP security models.
v2c	Specifies that the group is using the SNMPv2c security model. The SNMPv2c security model allows informs to be transmitted and supports 64-character strings.
v3	Specifies that the group is using the SNMPv3 security model. SMNPv3 is the most secure of the supported security models. It allows you to explicitly configure authentication characteristics.
auth	Specifies authentication of a packet without encrypting it.
noauth	Specifies no authentication of a packet.
priv	Specifies authentication of a packet with encryption.
context	(Optional) Specifies the SNMP context to associate with this SNMP group and its views.
context-name	(Optional) Context name.
match	(Optional) Specifies an exact context match or matches only the context prefix.
exact	(Optional) Matches the exact context.
prefix	(Optional) Matches only the context prefix.
read	(Optional) Specifies a read view for the SNMP group. This view enables you to view only the contents of the agent.
read-view	(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.
write	(Optional) Specifies a write view for the SNMP group. This view enables you to enter data and configure the contents of the agent.

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

Release	Modification
Cisco IOS XE Fuji 16.8.1a	This command was introduced.

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
```

```
Device(config)# snmp mib community-map commA context A target-list commAVpn
Device(config)# snmp-server group GROUP1 v2c context A read viewA write viewA notify viewB
```

Related Commands

Command	Description
show snmp group	Displays the names of groups on the device and the security model, the status of the different views, and the storage type of each group.
snmp mib community-map	Associates a SNMP community with an SNMP context, engine ID, security name, or VPN target list.
snmp-server host	Specifies the recipient of a SNMP notification operation.
snmp-server user	Configures a new user to a SNMP group.

snmp-server host

To specify the recipient (host) of a Simple Network Management Protocol (SNMP) notification operation, use the **snmp-server host** global configuration command on the device. Use the **no** form of this command to remove the specified host.

snmp-server host {*host-addr* } [**vrf** *vrf-instance*] [**informs** | **traps**] [**version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**} }] {*community-string* [*notification-type*] }
no snmp-server host {*host-addr* } [**vrf** *vrf-instance*] [**informs** | **traps**] [**version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**} }] {*community-string* [*notification-type*] }

Syntax Description

host-addr	Name or Internet address of the host (the targeted recipient).
vrf *vrf-instance*	(Optional) Specifies the virtual private network (VPN) routing instance and name for this host.
informs | **traps**	(Optional) Sends SNMP traps or informs to this host.
version 1 | **2c** | **3**	(Optional) Specifies the version of the SNMP used to send the traps. **1**—SNMPv1. This option is not available with informs. **2c**—SNMPv2C. **3**—SNMPv3. One of the authorization keywords (see next table row) must follow the Version 3 keyword.
auth | **noauth** | **priv**	**auth** (Optional)—Enables Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication. **noauth** (Default)—The noAuthNoPriv security level. This is the default if the **auth** | **noauth** | **priv** keyword choice is not specified. **priv** (Optional)—Enables Data Encryption Standard (DES) packet encryption (also called privacy).
community-string	Password-like community string sent with the notification operation. Though you can set this string by using the **snmp-server host** command, we recommend that you define this string by using the **snmp-server community** global configuration command before using the **snmp-server host** command. **Note** The @ symbol is used for delimiting the context information. Avoid using the @ symbol as part of the SNMP community string when configuring this command.

notification-type	(Optional) Type of notification to be sent to the host. If no type is specified, all notifications are sent. The notification type can be one or more of the these keywords: • **auth-framework**—Sends SNMP CISCO-AUTH-FRAMEWORK-MIB traps. • **bridge**—Sends SNMP Spanning Tree Protocol (STP) bridge MIB traps. • **bulkstat**—Sends Data-Collection-MIB Collection notification traps. • **call-home**—Sends SNMP CISCO-CALLHOME-MIB traps. • **cef**—Sends SNMP CEF traps. • **config**—Sends SNMP configuration traps. • **config-copy**—Sends SNMP config-copy traps. • **config-ctid**—Sends SNMP config-ctid traps. • **copy-config**—Sends SNMP copy configuration traps. • **cpu**—Sends CPU notification traps. • **cpu threshold**—Sends CPU threshold notification traps. • **entity**—Sends SNMP entity traps.

- **envmon**—Sends environmental monitor traps.
- **errdisable**—Sends SNMP errdisable notification traps.
- **event-manager**—Sends SNMP Embedded Event Manager traps.
- **flash**—Sends SNMP FLASH notifications.
- **flowmon**—Sends SNMP flowmon notification traps.
- **ipmulticast**—Sends SNMP IP multicast routing traps.
- **ipsla**—Sends SNMP IP SLA traps.
- **license**—Sends license traps.
- **local-auth**—Sends SNMP local auth traps.
- **mac-notification**—Sends SNMP MAC notification traps.
- **pim**—Sends SNMP Protocol-Independent Multicast (PIM) traps.
- **power-ethernet**—Sends SNMP power Ethernet traps.
- **snmp**—Sends SNMP-type traps.
- **storm-control**—Sends SNMP storm-control traps.
- **stpx**—Sends SNMP STP extended MIB traps.
- **syslog**—Sends SNMP syslog traps.
- **transceiver**—Sends SNMP transceiver traps.
- **tty**—Sends TCP connection traps.
- **vlan-membership**— Sends SNMP VLAN membership traps.
- **vlancreate**—Sends SNMP VLAN-created traps.
- **vlandelete**—Sends SNMP VLAN-deleted traps.
- **vrfmib**—Sends SNMP vrfmib traps.
- **vtp**—Sends SNMP VLAN Trunking Protocol (VTP) traps.
- **wireless**—Sends wireless traps.

Command Default

This command is disabled by default. No notifications are sent.

If you enter this command with no keywords, the default is to send all trap types to the host. No informs are sent to this host.

If no **version** keyword is present, the default is Version 1.

If Version 3 is selected and no authentication keyword is entered, the default is the **noauth** (noAuthNoPriv) security level.

Note Though visible in the command-line help strings, the **fru-ctrl** keyword is not supported.

Command Modes Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send acknowledgments when it receives traps. The sender cannot determine if the traps were received. However, an SNMP entity that receives an inform request acknowledges the message with an SNMP response PDU. If the sender never receives the response, the inform request can be sent again, so that informs are more likely to reach their intended destinations.

However, informs consume more resources in the agent and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Traps are also sent only once, but an inform might be retried several times. The retries increase traffic and contribute to a higher overhead on the network.

If you do not enter an **snmp-server host** command, no notifications are sent. To configure the device to send SNMP notifications, you must enter at least one **snmp-server host** command. If you enter the command with no keywords, all trap types are enabled for the host. To enable multiple hosts, you must enter a separate **snmp-server host** command for each host. You can specify multiple notification types in the command for each host.

If a local user is not associated with a remote host, the device does not send informs for the **auth** (authNoPriv) and the **priv** (authPriv) authentication levels.

When multiple **snmp-server host** commands are given for the same host and kind of notification (trap or inform), each succeeding command overwrites the previous command. Only the last **snmp-server host** command is in effect. For example, if you enter an **snmp-server host inform** command for a host and then enter another **snmp-server host inform** command for the same host, the second command replaces the first.

The **snmp-server host** command is used with the **snmp-server enable traps** global configuration command. Use the **snmp-server enable traps** command to specify which SNMP notifications are sent globally. For a host to receive most notifications, at least one **snmp-server enable traps** command and the **snmp-server host** command for that host must be enabled. Some notification types cannot be controlled with the **snmp-server enable traps** command. For example, some notification types are always enabled. Other notification types are enabled by a different command.

The **no snmp-server host** command with no keywords disables traps, but not informs, to the host. To disable informs, use the **no snmp-server host informs** command.

Examples

This example shows how to configure a unique SNMP community string named comaccess for traps and prevent SNMP polling access with this string through access-list 10:

```
Device(config)# snmp-server community comaccess ro 10
Device(config)# snmp-server host 172.20.2.160 comaccess
Device(config)# access-list 10 deny any
```

This example shows how to send the SNMP traps to the host specified by the name myhost.cisco.com. The community string is defined as comaccess:

```
Device(config)# snmp-server enable traps
Device(config)# snmp-server host myhost.cisco.com comaccess snmp
```

This example shows how to enable the device to send all traps to the host myhost.cisco.com by using the community string public:

```
Device(config)# snmp-server enable traps
Device(config)# snmp-server host myhost.cisco.com public
```

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

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-numberacl-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-numberacl-name*}]

Syntax Description

username	Name of the user on the host that connects to the agent.
group-name	Name of the group to which the user belongs.
remote	(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.
host	(Optional) Name or IP address of the remote SNMP host.
udp-port	(Optional) Specifies the User Datagram Protocol (UDP) port number of the remote host.
port	(Optional) Integer value that identifies the UDP port. The default is 162.
vrf	(Optional) Specifies an instance of a routing table.
vrf-name	(Optional) Name of the Virtual Private Network (VPN) routing and forwarding (VRF) table to use for storing data.
v1	Specifies that SNMPv1 should be used.
v2c	Specifies that SNMPv2c should be used.
v3	Specifies that the SNMPv3 security model should be used. Allows the use of the **encrypted** keyword or **auth** keyword or both.
encrypted	(Optional) Specifies whether the password appears in encrypted format.
auth	(Optional) Specifies which authentication level should be used.
md5	(Optional) Specifies the HMAC-MD5-96 authentication level.
sha	(Optional) Specifies the HMAC-SHA-96 authentication level.
auth-password	(Optional) String (not to exceed 64 characters) that enables the agent to receive packets from the host.
access	(Optional) Specifies an Access Control List (ACL) to be associated with this SNMP user.
ipv6	(Optional) Specifies an IPv6 named access list to be associated with this SNMP user.

nacl	(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.
priv	(Optional) Specifies the use of the User-based Security Model (USM) for SNMP version 3 for SNMP message level security.
des	(Optional) Specifies the use of the 56-bit Digital Encryption Standard (DES) algorithm for encryption.
3des	(Optional) Specifies the use of the 168-bit 3DES algorithm for encryption.
aes	(Optional) Specifies the use of the Advanced Encryption Standard (AES) algorithm for encryption.
128	(Optional) Specifies the use of a 128-bit AES algorithm for encryption.
192	(Optional) Specifies the use of a 192-bit AES algorithm for encryption.
256	(Optional) Specifies the use of a 256-bit AES algorithm for encryption.
privpassword	(Optional) String (not to exceed 64 characters) that specifies the privacy user password.
acl-number	(Optional) Integer in the range from 1 to 99 that specifies a standard access list of IP addresses.
acl-name	(Optional) String (not to exceed 64 characters) that is the name of a standard access list of IP addresses.

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

Release	Modification
Cisco IOS XE Fuji 16.8.1a	This command was introduced.

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 102: snmp-server user Default Descriptions

Characteristic	Default
Access lists	Access from all IP access lists is permitted.
Encryption	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.
Passwords	Assumed to be text strings.
Remote users	All users are assumed to be local to this SNMP engine unless you specify they are remote with the **remote** keyword.

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:

```
Device(config)# snmp-server user abcd public v3 encrypted auth md5
00:11:22:33:44:55:66:77:88:99:AA:BB:CC:DD:EE:FF
```

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

Command	Description
show running-config	Displays the contents of the currently running configuration file or the configuration for a specific interface, or map class information.
show snmp user	Displays information on each SNMP username in the group username table.
snmp-server engineID	Displays the identification of the local SNMP engine and all remote engines that have been configured on the device.

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.

snmp-server view *view-name oid-tree* {**included** | **excluded**}
no snmp-server view *view-name*

Syntax Description

view-name	Label for the view record that you are updating or creating. The name is used to reference the record.
oid-tree	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 (*) wildcard to specify a subtree family; for example 1.3.*.4.
included	Configures the OID (and subtree OIDs) specified in *oid-tree* argument to be included in the SNMP view.
excluded	Configures the OID (and subtree OIDs) specified in *oid-tree* argument to be explicitly excluded from the SNMP view.

Command Default

No view entry exists.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.8.1a	This command was introduced.

Usage Guidelines

Other SNMP commands require an SMP 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:

```
snmp-server view root_view system included
snmp-server view root_view cisco included
```

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

Command	Description
snmp-server community	Sets up the community access string to permit access to the SNMP protocol.
snmp-server manager	Starts the SNMP manager process.

switchport mode access

To sets the interface as a nontrunking nontagged single-VLAN Ethernet interface , use the **switchport mode access** command in template configuration mode. Use the **no** form of this command to return to the default setting.

switchport mode access
no switchport mode access

Syntax Description

switchport mode access	Sets the interface as a nontrunking nontagged single-VLAN Ethernet interface.

Command Default

An access port can carry traffic in one VLAN only. By default, an access port carries traffic for VLAN1.

Command Modes

Template configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Examples

This example shows how to set a single-VLAN interface

```
Device(config-template)# switchport mode access
```

switchport voice vlan

To specify to forward all voice traffic through the specified VLAN, use the **switchport voice vlan** command in template configuration mode. Use the **no** form of this command to return to the default setting.

switchport voice vlan*vlan_id*
no switchport voice vlan

Syntax Description

switchport voice vlan*vlan_id*	Specifies to forward all voice traffic through the specified VLAN.

Command Default

You can specify a value from 1 to 4094.

Command Modes

Template configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Examples

This example shows how to specify to forward all voice traffic through the specified VLAN.

```
Device(config-template)# switchport voice vlan 20
```

Flexible NetFlow Commands

- cache, on page 907
- clear flow exporter, on page 909
- clear flow monitor, on page 910
- collect, on page 912
- collect counter, on page 913
- collect interface, on page 914
- collect timestamp absolute, on page 915
- collect transport tcp flags, on page 916
- datalink flow monitor, on page 917
- debug flow exporter, on page 918
- debug flow monitor, on page 919
- debug flow record, on page 920
- debug sampler, on page 921
- description, on page 922
- destination, on page 923
- dscp, on page 924
- export-protocol netflow-v9, on page 925
- export-protocol netflow-v5, on page 926
- exporter, on page 927
- flow exporter, on page 928
- flow monitor, on page 929
- flow record, on page 930
- ip flow monitor, on page 931
- ipv6 flow monitor, on page 933
- match datalink dot1q priority, on page 935
- match datalink dot1q vlan, on page 936
- match datalink ethertype, on page 937
- match datalink mac, on page 938
- match datalink vlan, on page 939
- match flow cts, on page 940
- match flow direction, on page 941
- match interface, on page 942
- match ipv4, on page 943

- match ipv4 destination address, on page 944
- match ipv4 source address, on page 945
- match ipv4 ttl, on page 946
- match ipv6, on page 947
- match ipv6 destination address, on page 948
- match ipv6 hop-limit, on page 949
- match ipv6 source address, on page 950
- match transport, on page 951
- match transport icmp ipv4, on page 952
- match transport icmp ipv6, on page 953
- mode random 1 out-of, on page 954
- option, on page 955
- record, on page 957
- sampler, on page 958
- show flow exporter, on page 959
- show flow interface, on page 961
- show flow monitor, on page 963
- show flow record, on page 968
- show sampler, on page 969
- source, on page 971
- template data timeout, on page 973
- transport, on page 974
- ttl, on page 975

cache

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

cache {**timeout** {**active** | **inactive** | **update**} *seconds* | **type** **normal**}
no **cache** {**timeout** {**active** | **inactive** | **update**} | **type**}

Syntax Description

timeout	Specifies the flow timeout.
active	Specifies the active flow timeout.
inactive	Specifies the inactive flow timeout.
update	Specifies the update timeout for a permanent flow cache.
seconds	The timeout value in seconds. The range is 30 to 604800 (7 days) for a normal flow cache. For a permanent flow cache the range is 1 to 604800 (7 days).
type	Specifies the type of the flow cache.
normal	Configures a normal cache type. The entries in the flow cache will be aged out according to the **timeout active** *seconds* and **timeout inactive** *seconds* settings. This is the default cache type.

Command Default

The default flow monitor flow cache parameters are used.

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

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

Command Modes

Flow monitor configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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

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

The **cache timeout inactive** command also controls the aging behavior of the normal type of cache. If a flow has not seen any activity for a specified amount of time, that flow will be aged out. By default, this timeout is 15 seconds, but this value can be adjusted depending on the type of traffic expected. If a large number of short-lived flows is consuming many cache entries, reducing the inactive timeout can reduce this overhead. If a large number of flows frequently get aged out before they have finished collecting their data, increasing this timeout can result in better flow correlation. When you change the inactive flow timeout, the new timeout value takes effect immediately.

The **cache timeout update** command controls the periodic updates sent by the permanent type of cache. This behavior is similar to the active timeout, except that it does not result in the removal of the cache entry from the cache. By default, this timer value is 1800 seconds (30 minutes).

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

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

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

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

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

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

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

The following example shows how to configure the permanent cache update timeout:

```
Device(config)# flow monitor FLOW-MONITOR-1
Device(config-flow-monitor)# cache timeout update 5000
```

The following example shows how to configure a normal cache:

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

clear flow exporter

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

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

Syntax Description

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

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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

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

Examples

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

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

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

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

clear flow monitor

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

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

Syntax Description

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

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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

Note The statistics for the cleared cache entries are maintained.

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

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

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

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

Examples

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

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

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

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

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

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

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

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

collect

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

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

Syntax Description

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

Command Default

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

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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

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

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

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

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

collect counter

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

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

Syntax Description

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

Command Default

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

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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

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

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

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

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

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

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

collect interface

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

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

Syntax Description

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

Command Default

The input and output interface names are not configured as a non-key field.

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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

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

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

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

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

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

collect timestamp absolute

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

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

Syntax Description

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

Command Default

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

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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

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

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

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

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

collect transport tcp flags

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

collect transport tcp flags
no collect transport tcp flags

Syntax Description

This command has no arguments or keywords.

Command Default

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

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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

- **ack—**TCP acknowledgement flag
- **cwr—**TCP congestion window reduced flag
- **ece—**TCP ECN echo flag
- **fin—**TCP finish flag
- **psh—**TCP push flag
- **rst—**TCP reset flag
- **syn—**TCP synchronize flag
- **urg—**TCP urgent flag

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

The following example collects the TCP flags from a flow:

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

datalink flow monitor

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

datalink flow monitor *monitor-name* {**input** | **output** | **sampler** *sampler-name*}
no datalink flow monitor *monitor-name* {**input** | **output** | **sampler** *sampler-name*}

Syntax Description

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

Command Default

A flow monitor is not enabled.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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

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

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

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

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

debug flow exporter

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

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

Syntax Description

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

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Examples

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

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

debug flow monitor

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

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

Syntax Description

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

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Examples

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

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

debug flow record

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

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

Syntax Description

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

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Examples

The following example enables debugging for the flow record:

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

debug sampler

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

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

Syntax Description

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

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Examples

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

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

description

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

description *description*
no description *description*

Syntax Description

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

Command Default

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

Command Modes

The following command modes are supported:

Flow exporter configuration

Flow monitor configuration

Flow record configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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

The following example configures a description for a flow monitor:

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

destination

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

destination {*hostnameip-address*} **vrf** *vrf-label*
no destination {*hostnameip-address*} **vrf** *vrf-label*

Syntax Description

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

Command Default

An export destination is not configured.

Command Modes

Flow exporter configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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

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

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

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

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

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

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

dscp

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

dscp *dscp*
no dscp *dscp*

Syntax Description

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

Command Default

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

Command Modes

Flow exporter configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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

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

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

export-protocol netflow-v9

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

export-protocol netflow-v9

Syntax Description

This command has no arguments or keywords.

Command Default

NetFlow Version 9 is enabled.

Command Modes

Flow exporter configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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

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

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

export-protocol netflow-v5

To configure NetFlow Version 5 export as the export protocol for a Flexible NetFlow exporter, use the **export-protocol netflow-v5** command in flow exporter configuration mode.

export-protocol netflow-v5

Syntax Description

This command has no arguments or keywords.

Command Default

NetFlow Version 5 is enabled.

Command Modes

Flow exporter configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

exporter

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

exporter *exporter-name*
no exporter *exporter-name*

Syntax Description

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

Command Default

An exporter is not configured.

Command Modes

Flow monitor configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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

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

Examples

The following example configures an exporter for a flow monitor:

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

flow exporter

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

flow exporter *exporter-name*
no flow exporter *exporter-name*

Syntax Description

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

Command Default

Flexible NetFlow flow exporters are not present in the configuration.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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

Examples

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

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

flow monitor

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

flow monitor *monitor-name*
no flow monitor *monitor-name*

Syntax Description

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

Command Default

Flexible NetFlow flow monitors are not present in the configuration.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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

Examples

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

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

flow record

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

flow record *record-name*
no flow record *record-name*

Syntax Description

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

Command Default

A Flexible NetFlow flow record is not configured.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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

Examples

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

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

ip flow monitor

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

ip flow monitor *monitor-name* [**sampler** *sampler-name*] {**input** | **output**}
no ip flow monitor *monitor-name* [**sampler** *sampler-name*] {**input** | **output**}

Syntax Description

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

Command Default

A flow monitor is not enabled.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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

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

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

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

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

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

The following example enables the same flow monitor on the same interface for monitoring input and output traffic:

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

The following example enables two different flow monitors on the same interface for monitoring input and output traffic:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip flow monitor FLOW-MONITOR-1 input
Device(config-if)# ip flow monitor FLOW-MONITOR-2 output
```

The following example enables the same flow monitor on two different interfaces for monitoring input and output traffic:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip flow monitor FLOW-MONITOR-1 input
Device(config-if)# exit
Device(config)# interface gigabitethernet2/0/3
Device(config-if)# ip flow monitor FLOW-MONITOR-1 output
```

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

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

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

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

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

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

ipv6 flow monitor

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

ipv6 flow monitor *monitor-name* [**sampler** *sampler-name*] {**input** | **output**}
no ipv6 flow monitor *monitor-name* [**sampler** *sampler-name*] {**input** | **output**}

Syntax Description

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

Command Default

A flow monitor is not enabled.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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

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

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

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

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

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

The following example enables the same flow monitor on the same interface for monitoring input and output traffic:

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

The following example enables two different flow monitors on the same interface for monitoring input and output traffic:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ipv6 flow monitor FLOW-MONITOR-1 input
Device(config-if)# ipv6 flow monitor FLOW-MONITOR-2 output
```

The following example enables the same flow monitor on two different interfaces for monitoring input and output traffic:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ipv6 flow monitor FLOW-MONITOR-1 input
Device(config-if)# exit
Device(config)# interface gigabitethernet2/0/3
Device(config-if)# ipv6 flow monitor FLOW-MONITOR-1 output
```

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

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

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

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

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

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

match datalink dot1q priority

To configure the 802.1Q (dot1q) priority value as a key field for a flow record, use the **match datalink dot1q priority** command in flow record configuration mode. To disable the use of the priority as a key field for a flow record, use the **no** form of this command.

match datalink dot1q priority
no match datalink dot1q priority

Syntax Description

This command has no arguments or keywords.

Command Default

The priority field is not configured as a key field.

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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

The observation point of the **match datalink dot1q priority** command is the interface to which the flow monitor that contains the flow record with the command is applied.

The following example configures the 802.1Q priority as a key field for a flow record:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match datalink dot1q priority
```

match datalink dot1q vlan

To configure the 802.1Q (dot1q) VLAN value as a key field for a flow record, use the **match datalink dot1q vlan** command in flow record configuration mode. To disable the use of the 802.1Q VLAN value as a key field for a flow record, use the **no** form of this command.

match datalink dot1q vlan {**input** | **output**}
no match datalink dot1q vlan {**input** | **output**}

Syntax Description

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

Command Default

The 802.1Q VLAN ID is not configured as a key field.

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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

The input and output keywords of the **match datalink dot1q vlan** command are used to specify the observation point that is used by the **match datalink dot1q vlan** command to create flows based on the unique 802.1q VLAN IDs in the network traffic.

The following example configures the 802.1Q VLAN ID of traffic being received by the device as a key field for a flow record:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match datalink dot1q vlan input
```

match datalink ethertype

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

match datalink ethertype
no match datalink ethertype

Syntax Description

This command has no arguments or keywords.

Command Default

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

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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

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

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

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

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

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

match datalink mac

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

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

Syntax Description

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

Command Default

MAC addresses are not configured as a key field.

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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

The **input** and **output** keywords are used to specify the observation point that is used by the **match datalink mac** command to create flows based on the unique MAC addressees in the network traffic.

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

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

The following example configures the use of the source MAC addresses of packets that are transmitted by the device as a key field for a flow record:

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

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

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

match datalink vlan

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

match datalink vlan {**input** | **output**}
no match datalink vlan {**input** | **output**}

Syntax Description

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

Command Default

The VLAN ID is not configured as a key field.

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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

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

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

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

match flow cts

To configure CTS source group tag and destination group tag for a flow record, use the**match flow cts** command in flow record configuration mode. To disable the group tag as key field for a flow record, use the **no** form of this command.

match flow cts {**source** | **destination**} **group-tag**
no match flow cts {**source** | **destination**} **group-tag**

Syntax Description

cts destination group-tag	Configures the CTS destination field group as a key field.
cts source group-tag	Configures the CTS source field group as a key field.

Command Default

The CTS destination or source field group, flow direction and the flow sampler ID are not configured as key fields.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Policy inline configuration (config-if-policy-inline)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	The command was introduced.

Usage Guidelines

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

The following example configures the source group-tag as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match flow cts source group-tag
```

match flow direction

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

match flow direction
no match flow direction

Syntax Description

This command has no arguments or keywords.

Command Default

The flow direction is not configured as key fields.

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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

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

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

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

match interface

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

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

Syntax Description

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

Command Default

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

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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

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

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

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

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

match ipv4

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

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

Syntax Description

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

Command Default

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

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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

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

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

match ipv4 destination address

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

match ipv4 destination address
no match ipv4 destination address

Syntax Description

This command has no arguments or keywords.

Command Default

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

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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

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

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

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

match ipv4 source address

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

match ipv4 source address
no match ipv4 source address

Syntax Description

This command has no arguments or keywords.

Command Default

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

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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

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

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

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

match ipv4 ttl

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

match ipv4 ttl
no match ipv4 ttl

Syntax Description

This command has no arguments or keywords.

Command Default

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

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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

The following example configures IPv4 TTL as a key field:

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

match ipv6

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

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

Syntax Description

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

Command Default

The IPv6 fields are not configured as a key field.

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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

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

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

match ipv6 destination address

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

match ipv6 destination address
no match ipv6 destination address

Syntax Description

This command has no arguments or keywords.

Command Default

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

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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

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

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

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

match ipv6 hop-limit

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

match ipv6 hop-limit
no match ipv6 hop-limit

Syntax Description

This command has no arguments or keywords.

Command Default

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

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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

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

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

match ipv6 source address

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

match ipv6 source address
no match ipv6 source address

Syntax Description

This command has no arguments or keywords.

Command Default

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

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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

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

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

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

match transport

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

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

Syntax Description

destination-port	Configures the transport destination port as a key field.
icmp ipv4	Configures the ICMP IPv4 type field and the code field as key fields. For more information see, match transport icmp ipv4, on page 952.
icmp ipv6	Configures the ICMP IPv6 type field and the code field as key fields. For more information see, match transport icmp ipv6, on page 953.
igmp type	Configures time stamps based on the system uptime as a key field.
source-port	Configures the transport source port as a key field.

Command Default

The transport fields are not configured as a key field.

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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

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

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

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

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

match transport icmp ipv4

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

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

Syntax Description

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

Command Default

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

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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

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

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

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

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

match transport icmp ipv6

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

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

Syntax Description

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

Command Default

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

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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

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

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

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

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

mode random 1 out-of

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

mode random 1 out-of *window-size*
no mode

Syntax Description

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

Command Default

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

Command Modes

Sampler configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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

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

Examples

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

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

option

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

option {**exporter-stats** | **interface-table** | **sampler-table**} [{**timeout** *seconds*}]
no option {**exporter-stats** | **interface-table** | **sampler-table**}

Syntax Description

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

Command Default

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

Command Modes

Flow exporter configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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

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

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

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

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

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

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

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

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

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

record

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

record *record-name*
no record

Syntax Description

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

Command Default

A flow record is not configured.

Command Modes

Flow monitor configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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

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

Examples

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

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

sampler

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

sampler *sampler-name*
no sampler *sampler-name*

Syntax Description

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

Command Default

Flexible Netflow flow samplers are not configured.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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

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

Examples

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

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

show flow exporter

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

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

Syntax Description

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

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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

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

This table describes the significant fields shown in the display:

Table 103: show flow exporter Field Descriptions

Field	Description
Flow Exporter	The name of the flow exporter that you configured.
Description	The description that you configured for the exporter, or the default description User defined.
Transport Configuration	The transport configuration fields for this exporter.
Destination IP address	The IP address of the destination host.
Source IP address	The source IP address used by the exported packets.
Transport Protocol	The transport layer protocol used by the exported packets.
Destination Port	The destination UDP port to which the exported packets are sent.
Source Port	The source UDP port from which the exported packets are sent.
DSCP	The differentiated services code point (DSCP) value.
TTL	The time-to-live value.
Output Features	Specifies whether the **output-features** command, which causes the output features to be run on Flexible NetFlow export packets, has been used or not.

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

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

show flow interface

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

show flow interface [*type number*]

Syntax Description

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

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Examples

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

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

Interface Ethernet1/0
        monitor:         FLOW-MONITOR-1
        direction:       Output
        traffic(ip):     on
Device# show flow interface gigabitethernet1/0/2
Interface Ethernet0/0
        monitor:         FLOW-MONITOR-1
        direction:       Input
        traffic(ip):     sampler SAMPLER-2#
```

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

Table 104: show flow interface Field Descriptions

Field	Description
Interface	The interface to which the information applies.
monitor	The name of the flow monitor that is configured on the interface.
direction:	The direction of traffic that is being monitored by the flow monitor. The possible values are: • Input—Traffic is being received by the interface. • Output—Traffic is being transmitted by the interface.

Field	Description
traffic(ip)	Indicates if the flow monitor is in normal mode or sampler mode. The possible values are: • on—The flow monitor is in normal mode. • sampler—The flow monitor is in sampler mode (the name of the sampler will be included in the display).

show flow monitor

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

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

Syntax Description

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

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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

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

Examples

The following example displays the status for a flow monitor:

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

Flow Monitor FLOW-MONITOR-1:
  Description:       Used for basic traffic analysis
```

```
Flow Record:       flow-record-1
Flow Exporter:     flow-exporter-1
                   flow-exporter-2
Cache:
  Type:              normal
  Status:            allocated
  Size:              4096 entries / 311316 bytes
  Inactive Timeout:  15 secs
  Active Timeout:    1800 secs
  Update Timeout:    1800 secs
```

This table describes the significant fields shown in the display.

Table 105: show flow monitor monitor-name Field Descriptions

Field	Description
Flow Monitor	Name of the flow monitor that you configured.
Description	Description that you configured or the monitor, or the default description User defined.
Flow Record	Flow record assigned to the flow monitor.
Flow Exporter	Exporters that are assigned to the flow monitor.
Cache	Information about the cache for the flow monitor.
Type	Flow monitor cache type. The possible values are: • immediate—Flows are expired immediately. • normal—Flows are expired normally. • Permanent—Flows are never expired.
Status	Status of the flow monitor cache. The possible values are: • allocated—The cache is allocated. • being deleted—The cache is being deleted. • not allocated—The cache is not allocated.
Size	Current cache size.
Inactive Timeout	Current value for the inactive timeout in seconds.
Active Timeout	Current value for the active timeout in seconds.
Update Timeout	Current value for the update timeout in seconds.

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

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

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

DATALINK MAC SOURCE ADDRESS INPUT:       0000.0000.1000
DATALINK MAC DESTINATION ADDRESS INPUT:  6400.F125.59E6
IPV6 SOURCE ADDRESS:                     2001:DB8::1
IPV6 DESTINATION ADDRESS:                2001:DB8:1::1
TRNS SOURCE PORT:                        1111
TRNS DESTINATION PORT:                   2222
IP VERSION:                              6
IP PROTOCOL:                             6
IP TOS:                                  0x05
IP TTL:                                  11
tcp flags:                               0x20
counter bytes long:                      132059538
counter packets long:                    1158417
```

This table describes the significant fields shown in the display.

Table 106: show flow monitor monitor-name cache Field Descriptions

Field	Description
Cache type	Flow monitor cache type. The value is always normal, as it is the only supported cache type.
Cache Size	Number of entries in the cache.
Current entries	Number of entries in the cache that are in use.
Flows added	Flows added to the cache since the cache was created.
Flows aged	Flows expired from the cache since the cache was created.
Active timeout	Current value for the active timeout in seconds.
Inactive timeout	Current value for the inactive timeout in seconds.
DATALINK MAC SOURCE ADDRESS INPUT	MAC source address of input packets.
DATALINK MAC DESTINATION ADDRESS INPUT	MAC destination address of input packets.
IPV6 SOURCE ADDRESS	IPv6 source address.
IPV6 DESTINATION ADDRESS	IPv6 destination address.
TRNS SOURCE PORT	Source port for the transport protocol.
TRNS DESTINATION PORT	Destination port for the transport protocol.

Field	Description
IP VERSION	IP version.
IP PROTOCOL	Protocol number.
IP TOS	IP type of service (ToS) value.
IP TTL	IP time-to-live (TTL) value.
tcp flags	Value of the TCP flags.
counter bytes	Number of bytes that have been counted.
counter packets	Number of packets that have been counted.

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

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

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

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

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

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

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

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

```
counter bytes long:                     132059538
counter packets long:                   1158417
```

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

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

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

show flow record

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

show flow record [{**broker** [{**detail** | **picture**}] | [**name**] *record-name*}]

Syntax Description

broker	(Optional) Displays information about the state of the broker for the Flexible NetFlow flow record.
detail	(Optional) Displays detailed information about the flow record broker.
picture	(Optional) Displays a picture of the broker state.
name	(Optional) Specifies the name of a flow record.
record-name	(Optional) Name of a user-defined flow record that was previously configured.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

The following example displays the status and statistics for FLOW-RECORD-1:

```
Device# show flow record FLOW-RECORD-1
flow record FLOW-RECORD-1:
  Description:        User defined
  No. of users:       0
  Total field space:  24 bytes
  Fields:
    match ipv6 destination address
    match transport source-port
    collect interface input
```

show sampler

To display the status and statistics for a Flexible NetFlow sampler, use the **show sampler** command in privileged EXEC mode.

show sampler [{**broker** [{**detail** | **picture**}] | [**name**] *sampler-name*}]

Syntax Description

broker	(Optional) Displays information about the state of the broker for the Flexible NetFlow sampler.
detail	(Optional) Displays detailed information about the sampler broker.
picture	(Optional) Displays a picture of the broker state.
name	(Optional) Specifies the name of a sampler.
sampler-name	(Optional) Name of a sampler that was previously configured.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

The following example displays the status and statistics for all of the flow samplers configured:

```
Device# show sampler
Sampler SAMPLER-1:
  ID:             2083940135
  export ID:      0
  Description:    User defined
  Type:           Invalid (not in use)
  Rate:           1 out of 32
  Samples:        0
  Requests:       0
  Users (0):

Sampler SAMPLER-2:
  ID:             3800923489
  export ID:      1
  Description:    User defined
  Type:           random
  Rate:           1 out of 100
  Samples:        1
  Requests:       124
  Users (1):
    flow monitor FLOW-MONITOR-1 (datalink,vlan1)  0 out of 0
```

This table describes the significant fields shown in the display.

Table 107: show sampler Field Descriptions

Field	Description
ID	ID number of the flow sampler.
Export ID	ID of the flow sampler export.
Description	Description that you configured for the flow sampler, or the default description User defined.
Type	Sampling mode that you configured for the flow sampler.
Rate	Window size (for packet selection) that you configured for the flow sampler. The range is 2 to 32768.
Samples	Number of packets sampled since the flow sampler was configured or the device was restarted. This is equivalent to the number of times a positive response was received when the sampler was queried to determine if the traffic needed to be sampled. See the explanation of the Requests field in this table.
Requests	Number of times the flow sampler was queried to determine if the traffic needed to be sampled.
Users	Interfaces on which the flow sampler is configured.

source

To configure the source IP address interface for all of the packets sent by a Flexible Netflow flow exporter, use the **source** command in flow exporter configuration mode. To remove the source IP address interface for all of the packets sent by a Flexible Netflow flow exporter, use the **no** form of this command.

source *interface-type interface-number*
no source

Syntax Description

interface-type	Type of interface whose IP address you want to use for the source IP address of the packets sent by a Flexible Netflow flow exporter.
interface-number	Interface number whose IP address you want to use for the source IP address of the packets sent by a Flexible Netflow flow exporter.

Command Default

The IP address of the interface over which the Flexible Netflow datagram is transmitted is used as the source IP address.

Command Modes

Flow exporter configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The benefits of using a consistent IP source address for the datagrams that Flexible Netflow sends include the following:

- The source IP address of the datagrams exported by Flexible Netflow is used by the destination system to determine from which device the Flexible Netflow data is arriving. If your network has two or more paths that can be used to send Flexible Netflow datagrams from the device to the destination system and you do not specify the source interface from which the source IP address is to be obtained, the device uses the IP address of the interface over which the datagram is transmitted as the source IP address of the datagram. In this situation the destination system might receive Flexible Netflow datagrams from the same device , but with different source IP addresses. When the destination system receives Flexible Netflow datagrams from the same device with different source IP addresses, the destination system treats the Flexible Netflow datagrams as if they were being sent from different devices . To avoid having the destination system treat the Flexible Netflow datagrams as if they were being sent from different devices, you must configure the destination system to aggregate the Flexible Netflow datagrams it receives from all of the possible source IP addresses in the device into a single Flexible Netflow flow.
- If your device has multiple interfaces that can be used to transmit datagrams to the destination system, and you do not configure the **source** command, you will have to add an entry for the IP address of each interface into any access lists that you create for permitting Flexible Netflow traffic. Creating and maintaining access lists for permitting Flexible Netflow traffic from known sources and blocking it from unknown sources is easier when you limit the source IP address for Flexible Netflow datagrams to a single IP address for each device that is exporting Flexible Netflow traffic.

Caution The interface that you configure as the **source** interface must have an IP address configured, and it must be up.

Tip When a transient outage occurs on the interface that you configured with the **source** command, the Flexible Netflow exporter reverts to the default behavior of using the IP address of the interface over which the datagrams are being transmitted as the source IP address for the datagrams. To avoid this problem, use a loopback interface as the source interface because loopback interfaces are not subject to the transient outages that can occur on physical interfaces.

To return this command to its default settings, use the **no source** or **default source** flow exporter configuration command.

Examples

The following example shows how to configure Flexible Netflow to use a loopback interface as the source interface for NetFlow traffic:

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# source loopback 0
```

template data timeout

To specify a timeout period for resending flow exporter template data, use the **template data timeout** command in flow exporter configuration mode. To remove the template resend timeout for a flow exporter, use the **no** form of this command.

template data timeout *seconds*
no template data timeout *seconds*

Syntax Description

seconds	Timeout value in seconds. The range is 1 to 86400. The default is 600.

Command Default

The default template resend timeout for a flow exporter is 600 seconds.

Command Modes

Flow exporter configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Flow exporter template data describes the exported data records. Data records cannot be decoded without the corresponding template. The **template data timeout** command controls how often those templates are exported.

To return this command to its default settings, use the **no template data timeout** or **default template data timeout** flow record exporter command.

The following example configures resending templates based on a timeout of 1000 seconds:

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# template data timeout 1000
```

transport

To configure the transport protocol for a flow exporter for Flexible Netflow, use the **transport** command in flow exporter configuration mode. To remove the transport protocol for a flow exporter, use the **no** form of this command.

transport udp *udp-port*
no transport udp *udp-port*

Syntax Description

udp *udp-port*	Specifies User Datagram Protocol (UDP) as the transport protocol and the UDP port number.

Command Default

Flow exporters use UDP on port 9995.

Command Modes

Flow exporter configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

To return this command to its default settings, use the **no transport** or **default transport flow exporter** configuration command.

The following example configures UDP as the transport protocol and a UDP port number of 250:

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# transport udp 250
```

ttl

To configure the time-to-live (TTL) value, use the **ttl** command in flow exporter configuration mode. To remove the TTL value, use the **no** form of this command.

ttl *ttl*
no ttl *ttl*

Syntax Description

ttl	Time-to-live (TTL) value for exported datagrams. The range is 1 to 255. The default is 255.

Command Default

Flow exporters use a TTL of 255.

Command Modes

Flow exporter configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

To return this command to its default settings, use the **no ttl** or **default ttl** flow exporter configuration command.

The following example specifies a TTL of 15:

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# ttl 15
```

PART VIII

QoS

- QoS Commands, on page 979

QoS Commands

- auto qos classify, on page 980
- auto qos trust, on page 982
- auto qos video, on page 989
- auto qos voip , on page 999
- class, on page 1013
- class-map, on page 1015
- debug auto qos, on page 1017
- match (class-map configuration), on page 1018
- policy-map, on page 1021
- priority, on page 1023
- queue-buffers ratio, on page 1025
- queue-limit, on page 1026
- random-detect cos, on page 1028
- random-detect cos-based, on page 1029
- random-detect dscp, on page 1030
- random-detect dscp-based, on page 1032
- random-detect precedence, on page 1033
- random-detect precedence-based, on page 1035
- service-policy (Wired), on page 1036
- set, on page 1038
- show auto qos , on page 1044
- show class-map, on page 1046
- show platform hardware fed switch, on page 1047
- show platform software fed switch qos, on page 1050
- show platform software fed switch qos qsb, on page 1051
- show policy-map, on page 1054
- show tech-support qos, on page 1056
- trust device, on page 1058

auto qos classify

To automatically configure quality of service (QoS) classification for untrusted devices within a QoS domain, use the **auto qos classify** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

auto qos classify [**police**]
no auto qos classify [**police**]

Syntax Description

police	(Optional) Configure QoS policing for untrusted devices.

Command Default

Auto-QoS classify is disabled on the port.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	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-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)
- 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.

auto qos trust

To automatically configure quality of service (QoS) for trusted interfaces within a QoS domain, use the **auto qos trust** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

auto qos trust {**cos** | **dscp**}
no auto qos trust {**cos** | **dscp**}

Syntax Description

cos	Trusts the CoS packet classification.
dscp	Trusts the DSCP packet classification.

Command Default

Auto-QoS trust is disabled on the port.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Use this command to configure the QoS for trusted interfaces within the QoS domain. The QoS domain includes the device, the network interior, and edge devices that can classify incoming traffic for QoS. When auto-QoS is enabled, it uses the ingress packet label to categorize traffic, to assign packet labels, and to configure the ingress and egress queues.

Table 108: Traffic Types, Packet Labels, and Queues

	VOIP Data Traffic	VOIP Control Traffic	Routing Protocol Traffic	STP[2] BPDU[3] Traffic	Real-Time Video Traffic	All Other Traffic
DSCP[4]	46	24, 26	48	56	34	–
CoS[5]	5	3	6	7	3	–

[2] STP = Spanning Tree Protocol
[3] BPDU = bridge protocol data unit
[4] DSCP = Differentiated Services Code Point
[5] CoS = class of service

Note The device applies the auto-QoS-generated commands as if the commands were entered from the command-line interface (CLI). An existing user configuration can cause the application of the generated commands to fail or to be overridden by the generated commands. These actions occur without warning. If all the generated commands are successfully applied, any user-entered configuration that was not overridden remains in the running configuration. Any user-entered configuration that was overridden can be retrieved by reloading the device without saving the current configuration to memory. If the generated commands fail to be applied, the previous running configuration is restored.

After auto-QoS is enabled, do not modify a policy map or aggregate policer that includes *AutoQoS* in its name. If you need to modify the policy map or aggregate policer, make a copy of it, and change the copied policy map or policer. To use the new policy map instead of the generated one, remove the generated policy map from the interface, and apply the new policy map.

To display the QoS configuration that is automatically generated when auto-QoS is enabled, enable debugging before you enable auto-QoS. Use the **debug auto qos** privileged EXEC command to enable auto-QoS debugging.

The following policy maps and class maps are created and applied when running the **auto qos trust cos** command.

Policy maps:

- AutoQos-4.0-Trust-Cos-Input-Policy
- AutoQos-4.0-Output-Policy

Class maps:

- class-default (match-any)
- AutoQos-4.0-Output-Priority-Queue (match-any)
- AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
- AutoQos-4.0-Output-Trans-Data-Queue (match-any)
- AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
- AutoQos-4.0-Output-Scavenger-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)

The following policy maps and class maps are created and applied when running the **auto qos trust dscp** command:

Policy maps:

- AutoQos-4.0-Trust-Dscp-Input-Policy
- AutoQos-4.0-Output-Policy

Class maps:

- class-default (match-any)

- AutoQos-4.0-Output-Priority-Queue (match-any)
- AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
- AutoQos-4.0-Output-Trans-Data-Queue (match-any)
- AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
- AutoQos-4.0-Output-Scavenger-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)

To disable auto-QoS on a port, use the **no auto qos trust** interface configuration command. Only the auto-QoS-generated interface configuration commands for this port are removed. If this is the last port on which auto-QoS is enabled and you enter the **no auto qos trust** command, auto-QoS is considered disabled even though the auto-QoS-generated global configuration commands remain (to avoid disrupting traffic on other ports affected by the global configuration).

Examples

This example shows how to enable auto-QoS for a trusted interface with specific CoS classification.

```
Device(config)# interface gigabitethernet1/0/17
Device(config-if)# auto qos trust cos
Device(config-if)# end
Device# show policy-map interface gigabitethernet1/0/17

Gigabitethernet1/0/17

  Service-policy input: AutoQos-4.0-Trust-Cos-Input-Policy

    Class-map: class-default (match-any)
      0 packets
      Match: any
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        cos cos table AutoQos-4.0-Trust-Cos-Table

  Service-policy output: AutoQos-4.0-Output-Policy

    queue stats for all priority classes:
      Queueing
      priority level 1

      (total drops) 0
      (bytes output) 0

    Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
      0 packets
      Match:  dscp cs4 (32) cs5 (40) ef (46)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: cos  5
        0 packets, 0 bytes
        5 minute rate 0 bps
      Priority: 30% (300000 kbps), burst bytes 7500000,

      Priority Level: 1
```

```
Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
  0 packets
  Match:  dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  3
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing
  queue-limit dscp 16 percent 80
  queue-limit dscp 24 percent 90
  queue-limit dscp 48 percent 100
  queue-limit dscp 56 percent 100

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%

  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
  0 packets
  Match:  dscp af41 (34) af42 (36) af43 (38)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  4
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
  0 packets
  Match:  dscp af21 (18) af22 (20) af23 (22)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  2
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
  0 packets
  Match:  dscp af11 (10) af12 (12) af13 (14)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  1
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 4%
  queue-buffers ratio 10
```

```
  Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
    0 packets
    Match:  dscp cs1 (8)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 1%
    queue-buffers ratio 10

  Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
    0 packets
    Match:  dscp af31 (26) af32 (28) af33 (30)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 10%
    queue-buffers ratio 10

  Class-map: class-default (match-any)
    0 packets
    Match: any
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 25%
    queue-buffers ratio 25
```

This example shows how to enable auto-QoS for a trusted interface with specific DSCP classification.

```
Device(config)# interface gigabitethernet1/0/18
Device(config-if)# auto qos trust dscp
Device(config-if)# end
Device#show policy-map interface gigabitethernet1/0/18
GigabitEthernet1/0/18

  Service-policy input: AutoQos-4.0-Trust-Dscp-Input-Policy

    Class-map: class-default (match-any)
      0 packets
      Match: any
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        dscp dscp table AutoQos-4.0-Trust-Dscp-Table

  Service-policy output: AutoQos-4.0-Output-Policy

    queue stats for all priority classes:
      Queueing
      priority level 1

      (total drops) 0
```

```
  (bytes output) 0

Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
  0 packets
  Match:  dscp cs4 (32) cs5 (40) ef (46)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  5
    0 packets, 0 bytes
    5 minute rate 0 bps
  Priority: 30% (300000 kbps), burst bytes 7500000,

  Priority Level: 1

Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
  0 packets
  Match:  dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  3
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing
  queue-limit dscp 16 percent 80
  queue-limit dscp 24 percent 90
  queue-limit dscp 48 percent 100
  queue-limit dscp 56 percent 100

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%

  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
  0 packets
  Match:  dscp af41 (34) af42 (36) af43 (38)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  4
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
  0 packets
  Match:  dscp af21 (18) af22 (20) af23 (22)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  2
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10
```

```
Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
  0 packets
  Match:  dscp af11 (10) af12 (12) af13 (14)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  1
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 4%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
  0 packets
  Match:  dscp cs1 (8)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 1%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
  0 packets
  Match:  dscp af31 (26) af32 (28) af33 (30)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: class-default (match-any)
  0 packets
  Match: any
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 25%
  queue-buffers ratio 25
```

You can verify your settings by entering the **show auto qos interface** *interface-id* privileged EXEC command.

auto qos video

To automatically configure quality of service (QoS) for video within a QoS domain, use the **auto qos video** command in interface configuration mode. Use the **no** form of this command to return to the default setting.

auto qos video { **cts** | **ip-camera** | **media-player** }
no auto qos video { **cts** | **ip-camera** | **media-player** }

Syntax Description

cts	Specifies a port connected to a Cisco TelePresence System and automatically configures QoS for video.
ip-camera	Specifies a port connected to a Cisco IP camera and automatically configures QoS for video.
media-player	Specifies a port connected to a CDP-capable Cisco digital media player and automatically configures QoS for video.

Command Default

Auto-QoS video is disabled on the port.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Use this command to configure the QoS appropriate for video traffic within the QoS domain. The QoS domain includes the device, the network interior, and edge devices that can classify incoming traffic for QoS. When auto-QoS is enabled, it uses the ingress packet label to categorize traffic, to assign packet labels, and to configure the ingress and egress queues. For more information, see the queue tables at the end of this section.

Auto-QoS configures the device for video connectivity to a Cisco TelePresence system, a Cisco IP camera, or a Cisco digital media player.

To take advantage of the auto-QoS defaults, you should enable auto-QoS before you configure other QoS commands. You can fine-tune the auto-QoS configuration *after* you enable auto-QoS.

The device applies the auto-QoS-generated commands as if the commands were entered from the command-line interface (CLI). An existing user configuration can cause the application of the generated commands to fail or to be overridden by the generated commands. These actions occur without warning. If all the generated commands are successfully applied, any user-entered configuration that was not overridden remains in the running configuration. Any user-entered configuration that was overridden can be retrieved by reloading the device without saving the current configuration to memory. If the generated commands fail to be applied, the previous running configuration is restored.

If this is the first port on which you have enabled auto-QoS, the auto-QoS-generated global configuration commands are executed followed by the interface configuration commands. If you enable auto-QoS on another port, only the auto-QoS-generated interface configuration commands for that port are executed.

After auto-QoS is enabled, do not modify a policy map or aggregate policer that includes *AutoQoS* in its name. If you need to modify the policy map or aggregate policer, make a copy of it, and change the copied policy

map or policer. To use the new policy map instead of the generated one, remove the generated policy map from the interface, and apply the new policy map.

To display the QoS configuration that is automatically generated when auto-QoS is enabled, enable debugging before you enable auto-QoS. Use the **debug auto qos** privileged EXEC command to enable auto-QoS debugging.

The following policy maps and class maps are created and applied when running the **auto qos video cts** command:

Policy maps:

- AutoQos-4.0-Trust-Cos-Input-Policy
- AutoQos-4.0-Output-Policy

Class maps

- class-default (match-any)
- AutoQos-4.0-Output-Priority-Queue (match-any)
- AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
- AutoQos-4.0-Output-Trans-Data-Queue (match-any)
- AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
- AutoQos-4.0-Output-Scavenger-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)

The following policy maps and class maps are created and applied when running the **auto qos video ip-camera** command:

Policy maps:

- AutoQos-4.0-Trust-Dscp-Input-Policy
- AutoQos-4.0-Output-Policy

Class maps:

- class-default (match-any)
- AutoQos-4.0-Output-Priority-Queue (match-any)
- AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
- AutoQos-4.0-Output-Trans-Data-Queue (match-any)
- AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
- AutoQos-4.0-Output-Scavenger-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)

The following policy maps and class maps are created and applied when running the **auto qos video media-player** command:

Policy maps:

- AutoQos-4.0-Trust-Dscp-Input-Policy
- AutoQos-4.0-Output-Policy

Class maps:

- class-default (match-any)
- AutoQos-4.0-Output-Priority-Queue (match-any)
- AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
- AutoQos-4.0-Output-Trans-Data-Queue (match-any)
- AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
- AutoQos-4.0-Output-Scavenger-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)

To disable auto-QoS on a port, use the **no auto qos video** interface configuration command. Only the auto-QoS-generated interface configuration commands for this port are removed. If this is the last port on which auto-QoS is enabled, and you enter the **no auto qos video** command, auto-QoS is considered disabled even though the auto-QoS-generated global configuration commands remain (to avoid disrupting traffic on other ports affected by the global configuration).

Table 109: Traffic Types, Packet Labels, and Queues

	VOIP Data Traffic	VOIP Control Traffic	Routing Protocol Traffic	STP[6] BPDU[7] Traffic	Real-Time Video Traffic	All Other Traffic
DSCP[8]	46	24, 26	48	56	34	–
CoS[9]	5	3	6	7	3	–

6 STP = Spanning Tree Protocol
7 BPDU = bridge protocol data unit
8 DSCP = Differentiated Services Code Point
9 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 gigabitethernet1/0/12
Device(config-if)# auto qos video cts
Device(config-if)# end
Device# show policy-map interface gigabitethernet1/0/12
Gigabitethernet1/0/12
```

```
Service-policy input: AutoQos-4.0-Trust-Cos-Input-Policy

  Class-map: class-default (match-any)
    0 packets
    Match: any
      0 packets, 0 bytes
      5 minute rate 0 bps
    QoS Set
      cos cos table AutoQos-4.0-Trust-Cos-Table

Service-policy output: AutoQos-4.0-Output-Policy

  queue stats for all priority classes:
    Queueing
    priority level 1

    (total drops) 0
    (bytes output) 0

  Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
    0 packets
    Match:  dscp cs4 (32) cs5 (40) ef (46)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Match: cos  5
      0 packets, 0 bytes
      5 minute rate 0 bps
    Priority: 30% (300000 kbps), burst bytes 7500000,

    Priority Level: 1

  Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
    0 packets
    Match:  dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Match: cos  3
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing
    queue-limit dscp 16 percent 80
    queue-limit dscp 24 percent 90
    queue-limit dscp 48 percent 100
    queue-limit dscp 56 percent 100

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 10%

    queue-buffers ratio 10

  Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
    0 packets
    Match:  dscp af41 (34) af42 (36) af43 (38)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Match: cos  4
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 10%
```

```
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
  0 packets
  Match:  dscp af21 (18) af22 (20) af23 (22)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  2
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
  0 packets
  Match:  dscp af11 (10) af12 (12) af13 (14)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  1
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 4%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
  0 packets
  Match:  dscp cs1 (8)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 1%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
  0 packets
  Match:  dscp af31 (26) af32 (28) af33 (30)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: class-default (match-any)
  0 packets
  Match: any
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
```

```
    (bytes output) 0
    bandwidth remaining 25%
    queue-buffers ratio 25
```

The following is an example of the **auto qos video ip-camera** command and the applied policies and class maps:

```
Device(config)# interface gigabitethernet1/0/9
Device(config-if)# auto qos video ip-camera
Device(config-if)# end
Device# show policy-map interface gigabitethernet1/0/9

Gigabitethernet1/0/9

  Service-policy input: AutoQos-4.0-Trust-Dscp-Input-Policy

    Class-map: class-default (match-any)
      0 packets
      Match: any
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        dscp dscp table AutoQos-4.0-Trust-Dscp-Table

  Service-policy output: AutoQos-4.0-Output-Policy

    queue stats for all priority classes:
      Queueing
      priority level 1

      (total drops) 0
      (bytes output) 0

    Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
      0 packets
      Match:  dscp cs4 (32) cs5 (40) ef (46)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: cos  5
        0 packets, 0 bytes
        5 minute rate 0 bps
      Priority: 30% (300000 kbps), burst bytes 7500000,

      Priority Level: 1

    Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
      0 packets
      Match:  dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: cos  3
        0 packets, 0 bytes
        5 minute rate 0 bps
      Queueing
      queue-limit dscp 16 percent 80
      queue-limit dscp 24 percent 90
      queue-limit dscp 48 percent 100
      queue-limit dscp 56 percent 100

      (total drops) 0
      (bytes output) 0
```

```
  bandwidth remaining 10%

  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
  0 packets
  Match:  dscp af41 (34) af42 (36) af43 (38)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  4
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
  0 packets
  Match:  dscp af21 (18) af22 (20) af23 (22)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  2
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
  0 packets
  Match:  dscp af11 (10) af12 (12) af13 (14)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  1
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 4%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
  0 packets
  Match:  dscp cs1 (8)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 1%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
  0 packets
  Match:  dscp af31 (26) af32 (28) af33 (30)
```

```
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 10%
    queue-buffers ratio 10

  Class-map: class-default (match-any)
    0 packets
    Match: any
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 25%
    queue-buffers ratio 25
```

The following is an example of the **auto qos video media-player** command and the applied policies and class maps.

```
Device(config)# interface gigabitethernet1/0/7
Device(config-if)# auto qos video media-player
Device(config-if)# end
Device# show policy-map interface gigabitethernet1/0/7

interface gigabitethernet1/0/7

  Service-policy input: AutoQos-4.0-Trust-Dscp-Input-Policy

    Class-map: class-default (match-any)
      0 packets
      Match: any
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        dscp dscp table AutoQos-4.0-Trust-Dscp-Table

  Service-policy output: AutoQos-4.0-Output-Policy

    queue stats for all priority classes:
      Queueing
      priority level 1

      (total drops) 0
      (bytes output) 0

    Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
      0 packets
      Match:  dscp cs4 (32) cs5 (40) ef (46)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: cos  5
        0 packets, 0 bytes
        5 minute rate 0 bps
      Priority: 30% (300000 kbps), burst bytes 7500000,

      Priority Level: 1
```

```
Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
  0 packets
  Match:  dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  3
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing
  queue-limit dscp 16 percent 80
  queue-limit dscp 24 percent 90
  queue-limit dscp 48 percent 100
  queue-limit dscp 56 percent 100

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%

  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
  0 packets
  Match:  dscp af41 (34) af42 (36) af43 (38)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  4
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
  0 packets
  Match:  dscp af21 (18) af22 (20) af23 (22)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  2
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
  0 packets
  Match:  dscp af11 (10) af12 (12) af13 (14)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  1
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 4%
```

```
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
  0 packets
  Match:  dscp cs1 (8)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 1%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
  0 packets
  Match:  dscp af31 (26) af32 (28) af33 (30)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: class-default (match-any)
  0 packets
  Match: any
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 25%
  queue-buffers ratio 25
```

You can verify your settings by entering the **show auto qos video interface** *interface-id* privileged EXEC command.

auto qos voip

To automatically configure quality of service (QoS) for voice over IP (VoIP) within a QoS domain, use the **auto qos voip** command in interface configuration mode. Use the **no** form of this command to return to the default setting.

auto qos voip {**cisco-phone** | **cisco-softphone** | **trust**}
no auto qos voip {**cisco-phone** | **cisco-softphone** | **trust**}

Syntax Description

cisco-phone	Specifies a port connected to a Cisco IP phone, and automatically configures QoS for VoIP. The QoS labels of incoming packets are trusted only when the telephone is detected.
cisco-softphone	Specifies a port connected to a device running the Cisco SoftPhone, and automatically configures QoS for VoIP.
trust	Specifies a port connected to a trusted device, and automatically configures QoS for VoIP. The QoS labels of incoming packets are trusted. For nonrouted ports, the CoS value of the incoming packet is trusted. For routed ports, the DSCP value of the incoming packet is trusted.

Command Default

Auto-QoS is disabled on the port.

When auto-QoS is enabled, it uses the ingress packet label to categorize traffic, to assign packet labels, and to configure the ingress and egress queues.

Command Default

Interface configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Use this command to configure the QoS appropriate for VoIP traffic within the QoS domain. The QoS domain includes the device, the network interior, and edge devices that can classify incoming traffic for QoS.

Auto-QoS configures the device for VoIP with Cisco IP phones on device and routed ports and for devices running the Cisco SoftPhone application. These releases support only Cisco IP SoftPhone Version 1.3(3) or later. Connected devices must use Cisco Call Manager Version 4 or later.

To take advantage of the auto-QoS defaults, you should enable auto-QoS before you configure other QoS commands. You can fine-tune the auto-QoS configuration *after* you enable auto-QoS.

Note The device applies the auto-QoS-generated commands as if the commands were entered from the command-line interface (CLI). An existing user configuration can cause the application of the generated commands to fail or to be overridden by the generated commands. These actions occur without warning. If all the generated commands are successfully applied, any user-entered configuration that was not overridden remains in the running configuration. Any user-entered configuration that was overridden can be retrieved by reloading the device without saving the current configuration to memory. If the generated commands fail to be applied, the previous running configuration is restored.

If this is the first port on which you have enabled auto-QoS, the auto-QoS-generated global configuration commands are executed followed by the interface configuration commands. If you enable auto-QoS on another port, only the auto-QoS-generated interface configuration commands for that port are executed.

When you enter the **auto qos voip cisco-phone** interface configuration command on a port at the edge of the network that is connected to a Cisco IP phone, the device enables the trusted boundary feature. The device uses the Cisco Discovery Protocol (CDP) to detect the presence of a Cisco IP phone. When a Cisco IP phone is detected, the ingress classification on the port is set to trust the QoS label received in the packet. The device also uses policing to determine whether a packet is in or out of profile and to specify the action on the packet. If the packet does not have a DSCP value of 24, 26, or 46 or is out of profile, the device changes the DSCP value to 0. When a Cisco IP phone is absent, the ingress classification is set to not trust the QoS label in the packet. The policing is applied to those traffic matching the policy-map classification before the device enables the trust boundary feature.

- When you enter the **auto qos voip cisco-softphone** interface configuration command on a port at the edge of the network that is connected to a device running the Cisco SoftPhone, the device uses policing to decide whether a packet is in or out of profile and to specify the action on the packet. If the packet does not have a DSCP value of 24, 26, or 46 or is out of profile, the device changes the DSCP value to 0.
- When you enter the **auto qos voip trust** interface configuration command on a port connected to the network interior, the device trusts the CoS value for nonrouted ports or the DSCP value for routed ports in ingress packets (the assumption is that traffic has already been classified by other edge devices).

You can enable auto-QoS on static, dynamic-access, and voice VLAN access, and trunk ports. When enabling auto-QoS with a Cisco IP phone on a routed port, you must assign a static IP address to the IP phone.

Note When a device running Cisco SoftPhone is connected to a device or routed port, the device supports only one Cisco SoftPhone application per port.

After auto-QoS is enabled, do not modify a policy map or aggregate policer that includes *AutoQoS* in its name. If you need to modify the policy map or aggregate policer, make a copy of it, and change the copied policy map or policer. To use the new policy map instead of the generated one, remove the generated policy map from the interface, and apply the new policy map.

To display the QoS configuration that is automatically generated when auto-QoS is enabled, enable debugging before you enable auto-QoS. Use the **debug auto qos** privileged EXEC command to enable auto-QoS debugging.

The following policy maps and class maps are created and applied when running the **auto qos voip trust** command:

Policy maps:

- AutoQos-4.0-Trust-Cos-Input-Policy
- AutoQos-4.0-Output-Policy

Class maps:

- class-default (match-any)
- AutoQos-4.0-Output-Priority-Queue (match-any)
- AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
- AutoQos-4.0-Output-Trans-Data-Queue (match-any)
- AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
- AutoQos-4.0-Output-Scavenger-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)

The following policy maps and class maps are created and applied when running the **auto qos voip cisco-softphone** command:

Policy maps:

- AutoQos-4.0-CiscoSoftPhone-Input-Policy
- AutoQos-4.0-Output-Policy

Class maps:

- AutoQos-4.0-Voip-Data-Class (match-any)
- AutoQos-4.0-Voip-Signal-Class (match-any)
- AutoQos-4.0-Multimedia-Conf-Class (match-any)
- AutoQos-4.0-Bulk-Data-Class (match-any)
- AutoQos-4.0-Transaction-Class (match-any)
- AutoQos-4.0-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)

- AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)

The following policy maps and class maps are created and applied when running the **auto qos voip cisco-phone** command:

Policy maps:

- service-policy input AutoQos-4.0-CiscoPhone-Input-Policy
- service-policy output AutoQos-4.0-Output-Policy

Class maps:

- class AutoQos-4.0-Voip-Data-CiscoPhone-Class
- class AutoQos-4.0-Voip-Signal-CiscoPhone-Class
- class AutoQos-4.0-Default-Class

To disable auto-QoS on a port, use the **no auto qos voip** interface configuration command. Only the auto-QoS-generated interface configuration commands for this port are removed. If this is the last port on which auto-QoS is enabled and you enter the **no auto qos voip** command, auto-QoS is considered disabled even though the auto-QoS-generated global configuration commands remain (to avoid disrupting traffic on other ports affected by the global configuration).

The device configures egress queues on the port according to the settings in this table.

Table 110: Auto-QoS Configuration for the Egress Queues

Egress Queue	Queue Number	CoS-to-Queue Map	Queue Weight (Bandwidth)	Queue (Buffer) Size for Gigabit-Capable Ports	Queue (Buffer) Size for 10/100 Ethernet Ports
Priority (shaped)	1	4, 5	Up to 100 percent	25 percent	15 percent
SRR shared	2	2, 3, 6, 7	10 percent	25 percent	25 percent
SRR shared	3	0	60 percent	25 percent	40 percent
SRR shared	4	1	20 percent	25 percent	20 percent

Examples

The following is an example of the **auto qos voip trust** command and the applied policies and class maps:

```
Device(config)# interface gigabitethernet1/0/31
Device(config-if)# auto qos voip trust
Device(config-if)# end
Device# show policy-map interface gigabitethernet1/0/31

Gigabitethernet1/0/31

  Service-policy input: AutoQos-4.0-Trust-Cos-Input-Policy

    Class-map: class-default (match-any)
      0 packets
```

```
    Match: any
      0 packets, 0 bytes
      5 minute rate 0 bps
    QoS Set
      cos cos table AutoQos-4.0-Trust-Cos-Table

Service-policy output: AutoQos-4.0-Output-Policy

  queue stats for all priority classes:
    Queueing
    priority level 1

    (total drops) 0
    (bytes output) 0

  Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
    0 packets
    Match:  dscp cs4 (32) cs5 (40) ef (46)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Match: cos  5
      0 packets, 0 bytes
      5 minute rate 0 bps
    Priority: 30% (300000 kbps), burst bytes 7500000,

    Priority Level: 1

  Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
    0 packets
    Match:  dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Match: cos  3
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing
    queue-limit dscp 16 percent 80
    queue-limit dscp 24 percent 90
    queue-limit dscp 48 percent 100
    queue-limit dscp 56 percent 100

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 10%

    queue-buffers ratio 10

  Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
    0 packets
    Match:  dscp af41 (34) af42 (36) af43 (38)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Match: cos  4
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 10%
    queue-buffers ratio 10

  Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
    0 packets
```

```
  Match:  dscp af21 (18) af22 (20) af23 (22)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  2
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
  0 packets
  Match:  dscp af11 (10) af12 (12) af13 (14)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  1
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 4%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
  0 packets
  Match:  dscp cs1 (8)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 1%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
  0 packets
  Match:  dscp af31 (26) af32 (28) af33 (30)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: class-default (match-any)
  0 packets
  Match: any
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 25%
  queue-buffers ratio 25
```

The following is an example of the **auto qos voip cisco-phone** command and the applied policies and class maps:

```
Device(config)# interface gigabitethernet1/0/5
Device(config-if)# auto qos voip cisco-phone
Device(config-if)# end
Device# show policy-map interface gigabitethernet1/0/5

Gigabitethernet1/0/5

  Service-policy input: AutoQos-4.0-CiscoPhone-Input-Policy

    Class-map: AutoQos-4.0-Voip-Data-CiscoPhone-Class (match-any)
      0 packets
      Match: cos  5
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        dscp ef
      police:
          cir 128000 bps, bc 8000 bytes
        conformed 0 bytes; actions:
          transmit
        exceeded 0 bytes; actions:
          set-dscp-transmit dscp table policed-dscp
        conformed 0000 bps, exceed 0000 bps

    Class-map: AutoQos-4.0-Voip-Signal-CiscoPhone-Class (match-any)
      0 packets
      Match: cos  3
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        dscp cs3
      police:
          cir 32000 bps, bc 8000 bytes
        conformed 0 bytes; actions:
          transmit
        exceeded 0 bytes; actions:
          set-dscp-transmit dscp table policed-dscp
        conformed 0000 bps, exceed 0000 bps

    Class-map: AutoQos-4.0-Default-Class (match-any)
      0 packets
      Match: access-group name AutoQos-4.0-Acl-Default
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        dscp default

    Class-map: class-default (match-any)
      0 packets
      Match: any
        0 packets, 0 bytes
        5 minute rate 0 bps

  Service-policy output: AutoQos-4.0-Output-Policy

    queue stats for all priority classes:
      Queueing
      priority level 1

      (total drops) 0
```

```
  (bytes output) 0

Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
  0 packets
  Match:  dscp cs4 (32) cs5 (40) ef (46)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  5
    0 packets, 0 bytes
    5 minute rate 0 bps
  Priority: 30% (300000 kbps), burst bytes 7500000,

  Priority Level: 1

Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
  0 packets
  Match:  dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  3
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing
  queue-limit dscp 16 percent 80
  queue-limit dscp 24 percent 90
  queue-limit dscp 48 percent 100
  queue-limit dscp 56 percent 100

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%

  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
  0 packets
  Match:  dscp af41 (34) af42 (36) af43 (38)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  4
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
  0 packets
  Match:  dscp af21 (18) af22 (20) af23 (22)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  2
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10
```

```
    Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
      0 packets
      Match:  dscp af11 (10) af12 (12) af13 (14)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: cos  1
        0 packets, 0 bytes
        5 minute rate 0 bps
      Queueing

      (total drops) 0
      (bytes output) 0
      bandwidth remaining 4%
      queue-buffers ratio 10

    Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
      0 packets
      Match:  dscp cs1 (8)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Queueing

      (total drops) 0
      (bytes output) 0
      bandwidth remaining 1%
      queue-buffers ratio 10

    Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
      0 packets
      Match:  dscp af31 (26) af32 (28) af33 (30)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Queueing

      (total drops) 0
      (bytes output) 0
      bandwidth remaining 10%
      queue-buffers ratio 10

    Class-map: class-default (match-any)
      0 packets
      Match: any
        0 packets, 0 bytes
        5 minute rate 0 bps
      Queueing

      (total drops) 0
      (bytes output) 0
      bandwidth remaining 25%
      queue-buffers ratio 25
```

The following is an example of the **auto qos voip cisco-softphone** command and the applied policies and class maps:

```
Device(config)# interface gigabitethernet1/0/20
Device(config-if)# auto qos voip cisco-softphone
Device(config-if)# end
Device# show policy-map interface gigabitethernet1/0/20

Gigabitethernet1/0/20

  Service-policy input: AutoQos-4.0-CiscoSoftPhone-Input-Policy
```

```
Class-map: AutoQos-4.0-Voip-Data-Class (match-any)
  0 packets
  Match:  dscp ef (46)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  5
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp ef
  police:
      cir 128000 bps, bc 8000 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      set-dscp-transmit dscp table policed-dscp
    conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Voip-Signal-Class (match-any)
  0 packets
  Match:  dscp cs3 (24)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  3
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp cs3
  police:
      cir 32000 bps, bc 8000 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      set-dscp-transmit dscp table policed-dscp
    conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Multimedia-Conf-Class (match-any)
  0 packets
  Match: access-group name AutoQos-4.0-Acl-MultiEnhanced-Conf
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp af41
  police:
      cir 5000000 bps, bc 156250 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      drop
    conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Bulk-Data-Class (match-any)
  0 packets
  Match: access-group name AutoQos-4.0-Acl-Bulk-Data
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp af11
  police:
      cir 10000000 bps, bc 312500 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
```

```
      set-dscp-transmit dscp table policed-dscp
    conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Transaction-Class (match-any)
  0 packets
  Match: access-group name AutoQos-4.0-Acl-Transactional-Data
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp af21
  police:
      cir 10000000 bps, bc 312500 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      set-dscp-transmit dscp table policed-dscp
    conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Scavanger-Class (match-any)
  0 packets
  Match: access-group name AutoQos-4.0-Acl-Scavanger
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp cs1
  police:
      cir 10000000 bps, bc 312500 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      drop
    conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Signaling-Class (match-any)
  0 packets
  Match: access-group name AutoQos-4.0-Acl-Signaling
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp cs3
  police:
      cir 32000 bps, bc 8000 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      drop
    conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Default-Class (match-any)
  0 packets
  Match: access-group name AutoQos-4.0-Acl-Default
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp default
  police:
      cir 10000000 bps, bc 312500 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      set-dscp-transmit dscp table policed-dscp
    conformed 0000 bps, exceed 0000 bps

Class-map: class-default (match-any)
```

```
    0 packets
    Match: any
      0 packets, 0 bytes
      5 minute rate 0 bps

Service-policy output: AutoQos-4.0-Output-Policy

  queue stats for all priority classes:
    Queueing
    priority level 1

    (total drops) 0
    (bytes output) 0

  Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
    0 packets
    Match:  dscp cs4 (32) cs5 (40) ef (46)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Match: cos  5
      0 packets, 0 bytes
      5 minute rate 0 bps
    Priority: 30% (300000 kbps), burst bytes 7500000,

    Priority Level: 1

  Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
    0 packets
    Match:  dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Match: cos  3
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing
    queue-limit dscp 16 percent 80
    queue-limit dscp 24 percent 90
    queue-limit dscp 48 percent 100
    queue-limit dscp 56 percent 100

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 10%

    queue-buffers ratio 10

  Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
    0 packets
    Match:  dscp af41 (34) af42 (36) af43 (38)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Match: cos  4
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 10%
    queue-buffers ratio 10

  Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
    0 packets
    Match:  dscp af21 (18) af22 (20) af23 (22)
```

```
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  2
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
  0 packets
  Match:  dscp af11 (10) af12 (12) af13 (14)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  1
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 4%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
  0 packets
  Match:  dscp cs1 (8)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 1%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
  0 packets
  Match:  dscp af31 (26) af32 (28) af33 (30)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: class-default (match-any)
  0 packets
  Match: any
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 25%
  queue-buffers ratio 25
```

You can verify your settings by entering the **show auto qos interface** *interface-id* privileged EXEC command.

class

To define a traffic classification match criteria for the specified class-map name, use the **class** command in policy-map configuration mode. Use the **no** form of this command to delete an existing class map.

class {*class-map-name* | **class-default**}
no class {*class-map-name* | **class-default**}

Syntax Description

class-map-name	The class map name.
class-default	Refers to a system default class that matches unclassified packets.

Command Default

No policy map class-maps are defined.

Command Modes

Policy-map configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Before using the **class** command, you must use the **policy-map** global configuration command to identify the policy map and enter policy-map configuration mode. After specifying a policy map, you can configure a policy for new classes or modify a policy for any existing classes in that policy map. You attach the policy map to a port by using the **service-policy** interface configuration command.

After entering the **class** command, you enter the policy-map class configuration mode. These configuration commands are available:

- **admit**—Admits a request for Call Admission Control (CAC)
- **bandwidth**—Specifies the bandwidth allocated to the class.
- **exit**—Exits the policy-map class configuration mode and returns to policy-map configuration mode.
- **no**—Returns a command to its default setting.
- **police**—Defines a policer or aggregate policer for the classified traffic. The policer specifies the bandwidth limitations and the action to take when the limits are exceeded. For more information about this command, see *Cisco IOS Quality of Service Solutions Command Reference* available on Cisco.com.
- **priority**—Assigns scheduling priority to a class of traffic belonging to a policy map.
- **queue-buffers**—Configures the queue buffer for the class.
- **queue-limit**—Specifies the maximum number of packets the queue can hold for a class policy configured in a policy map.
- **service-policy**—Configures a QoS service policy.
- **set**—Specifies a value to be assigned to the classified traffic. For more information, see 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 criterias 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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Use this command to specify the name of the class for which you want to create or modify class-map match criteria and to enter class-map configuration mode.

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).

Note You cannot configure IPv4 and IPv6 classification criteria simultaneously in the same class-map. However, they can be configured in different class-maps in the same policy.

Examples

This example shows how to configure the class map called class1 with one match criterion, which is an access list called 103:

```
Device(config)# access-list 103 permit ip any any dscp 10
Device(config)# class-map class1
Device(config-cmap)# match access-group 103
Device(config-cmap)# exit
```

This example shows how to delete the class map class1:

```
Device(config)# no class-map class1
```

You can verify your settings by entering the **show class-map** privileged EXEC command.

debug auto qos

To enable debugging of the automatic quality of service (auto-QoS) feature, use the **debug auto qos** command in privileged EXEC mode. Use the **no** form of this command to disable debugging.

debug auto qos
no debug auto qos

Syntax Description

This command has no arguments or keywords.

Command Default

Auto-QoS debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

To display the QoS configuration that is automatically generated when auto-QoS is enabled, enable debugging before you enable auto-QoS. You enable debugging by entering the **debug auto qos** privileged EXEC command.

The **undebug auto qos** command is the same as the **no debug auto qos** command.

When you enable debugging on a device stack, it is enabled only on the active device. To enable debugging on a stack member, you can start a session from the active device by using the **session** *switch-number* privileged EXEC command. Then enter the **debug** command at the command-line prompt of the stack member. You also can use the **remote command** *stack-member-number LINE* privileged EXEC command on the active device to enable debugging on a member device without first starting a session.

Examples

This example shows how to display the QoS configuration that is automatically generated when auto-QoS is enabled:

```
Device# debug auto qos
AutoQoS debugging is on
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# interface gigabitethernet 2/0/1
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

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

match {**access-group**{**name** *acl-name acl-index*} | **cos** *cos-value* | **dscp** *dscp-value* | [**ip**] **dscp** *dscp-list* | [**ip**] **precedence** *ip-precedence-list* | **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* | **non-client-nrt** | **precedence** *precedence-value1...value4* | **protocol** *protocol-name* | **qos-group** *qos-group-value* | **vlan** *vlan-id* | **wlan** *wlan-id*}

Syntax Description

access-group	Specifies an access group.
name *acl-name*	Specifies the name of an IP standard or extended access control list (ACL) or MAC ACL.
acl-index	Specifies the number of an IP standard or extended access control list (ACL) or MAC ACL. For an IP standard ACL, the ACL index range is 1 to 99 and 1300 to 1999. For an IP extended ACL, the ACL index range is 100 to 199 and 2000 to 2699.
class-map *class-map-name*	Uses a traffic class as a classification policy and specifies a traffic class name to use as the match criterion.
cos *cos-value*	Matches a packet on the basis of a Layer 2 class of service (CoS)/Inter-Switch Link (ISL) marking. The cos-value is from 0 to 7. You can specify up to four CoS values in one **match cos** statement, separated by a space.
dscp *dscp-value*	Specifies the parameters for each DSCP value. You can specify a value in the range 0 to 63 specifying the differentiated services code point value.

ip dscp *dscp-list*	Specifies a list of up to eight IP Differentiated Services Code Point (DSCP) values to match against incoming packets. Separate each value with a space. The range is 0 to 63. You also can enter a mnemonic name for a commonly used value.
ip precedence *ip-precedence-list*	Specifies a list of up to eight IP-precedence values to match against incoming packets. Separate each value with a space. The range is 0 to 7. You also can enter a mnemonic name for a commonly used value.
precedence *precedence-value1...value4*	Assigns an IP precedence value to the classified traffic. The range is 0 to 7. You also can enter a mnemonic name for a commonly used value.
qos-group *qos-group-value*	Identifies a specific QoS group value as a match criterion. The range is 0 to 31.
vlan *vlan-id*	Identifies a specific VLAN as a match criterion. The range is 1 to 4094.
non-client-nrt	Matches a non-client NRT (non-real-time).
protocol *protocol-name*	Specifies the type of protocol.
wlan *wlan-id*	Identifies 802.11 specific values.

Command Default

No match criteria are defined.

Command Modes

Class-map configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introc

Usage Guidelines

The **match** command is used to specify which fields in the incoming packets are examined to classify the packets. Only the IP access group or the MAC access group matching to the Ether Type/Len are supported.

If you enter the **class-map match-any***class-map-name* global configuration command, you can enter the following **match** commands:

- **match access-group name** *acl-name*

Note The ACL must be an extended named ACL.

- **match ip dscp** *dscp-list*
- **match ip precedence** *ip-precedence-list*

The **match access-group** *acl-index* command is not supported.

To define packet classification on a physical-port basis, only one **match** command per class map is supported. In this situation, the **match-any** keyword is equivalent.

For the **match ip dscp** *dscp-list* or the **match ip precedence** *ip-precedence-list* command, you can enter a mnemonic name for a commonly used value. For example, you can enter the **match ip dscp af11** command, which is the same as entering the **match ip dscp 10** command. You can enter the **match ip precedence critical** command, which is the same as entering the **match ip precedence 5** command. For a list of supported mnemonics, enter the **match ip dscp ?** or the **match ip precedence ?** command to see the command-line help strings.

Use the **input-interface** *interface-id-list* keyword when you are configuring an interface-level class map in a hierarchical policy map. For the *interface-id-list*, you can specify up to six entries.

Examples

This example shows how to create a class map called class2, which matches all the incoming traffic with DSCP values of 10, 11, and 12:

```
Device(config)# class-map class2
Device(config-cmap)# match ip dscp 10 11 12
Device(config-cmap)# exit
```

This example shows how to create a class map called class3, which matches all the incoming traffic with IP-precedence values of 5, 6, and 7:

```
Device(config)# class-map class3
Device(config-cmap)# match ip precedence 5 6 7
Device(config-cmap)# exit
```

This example shows how to delete the IP-precedence match criteria and to classify traffic using acl1:

```
Device(config)# class-map class2
Device(config-cmap)# match ip precedence 5 6 7
Device(config-cmap)# no match ip precedence
Device(config-cmap)# match access-group acl1
Device(config-cmap)# exit
```

This example shows how to specify a list of physical ports to which an interface-level class map in a hierarchical policy map applies:

```
Device(config)# class-map match-any class4
Device(config-cmap)# match cos 4
Device(config-cmap)# exit
```

This example shows how to specify a range of physical ports to which an interface-level class map in a hierarchical policy map applies:

```
Device(config)# class-map match-any class4
Device(config-cmap)# match cos 4
Device(config-cmap)# exit
```

You can verify your settings by entering the **show class-map** privileged EXEC command.

policy-map

To create or modify a policy map that can be attached to multiple physical ports or switch virtual interfaces (SVIs) and to enter policy-map configuration mode, use the **policy-map** command in global configuration mode. Use the **no** form of this command to delete an existing policy map and to return to global configuration mode.

policy-map *policy-map-name*
no policy-map *policy-map-name*

Syntax Description

policy-map-name	Name of the policy map.

Command Default

No policy maps are defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	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 show you how to configure hierarchical polices:

```
Device# configure terminal
Device(config)# class-map c1
Device(config-cmap)# exit

Device(config)# class-map c2
Device(config-cmap)# exit

Device(config)# policy-map child
Device(config-pmap)# class c1
Device(config-pmap-c)# priority level 1
Device(config-pmap-c)# police rate percent 20 conform-action transmit exceed action drop
Device(config-pmap-c-police)# exit
Device(config-pmap-c)# exit

Device(config-pmap)# class c2
Device(config-pmap-c)# bandwidth 20000
Device(config-pmap-c)# exit

Device(config-pmap)# class class-default
Device(config-pmap-c)# bandwidth 20000
Device(config-pmap-c)# exit
Device(config-pmap)# exit

Device(config)# policy-map parent
Device(config-pmap)# class class-default
Device(config-pmap-c)# shape average 1000000
Device(config-pmap-c)# service-policy child
Deviceconfig-pmap-c)# end
```

This example shows how to delete a policy map:

```
Device(config)# no policy-map policymap2
```

You can verify your settings by entering the **show policy-map** privileged EXEC command.

priority

To assign priority to a class of traffic belonging to a policy map, use the **priority** command in policy-map class configuration mode. To remove a previously specified priority for a class, use the **no** form of this command.

priority [*Kbps* [*burst -in-bytes*] | **level** *level-value* [*Kbps* [*burst -in-bytes*]] | **percent** *percentage* [*Kb/s* [*burst -in-bytes*]]]
no priority [*Kb/s* [*burst -in-bytes*] | **level** *level value* [*Kb/s* [*burst -in-bytes*]] | **percent** *percentage* [*Kb/s* [*burst -in-bytes*]]]

Syntax Description

Kb/s	(Optional) Guaranteed allowed bandwidth, in kilobits per second (kbps), for the priority traffic. The amount of guaranteed bandwidth varies according to the interface and platform in use. Beyond the guaranteed bandwidth, the priority traffic will be dropped in the event of congestion to ensure that the nonpriority traffic is not starved. The value must be between 1 and 2,000,000 kbps.
burst -in-bytes	(Optional) Burst size in bytes. The burst size configures the network to accommodate temporary bursts of traffic. The default burst value, which is computed as 200 milliseconds of traffic at the configured bandwidth rate, is used when the burst argument is not specified. The range of the burst is from 32 to 2000000 bytes.
level *level-value*	(Optional) Assigns priority level. Available values for *level-value* are 1 and 2. Level 1 is a higher priority than Level 2. Level 1 reserves bandwidth and goes first, so latency is very low.
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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Either the **bandwidth**, **shape**, or **priority** command must be used before using this command. For more information about these commands, see *Cisco IOS Quality of Service Solutions Command Reference* available on Cisco.com

The 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)# 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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Although visible in the command line help-strings, the **packets** unit of measure is not supported; use the **percent** unit of measure.

Note This command is supported only on wired ports in the egress direction.

Weighted fair queuing (WFQ) creates a queue for every class for which a class map is defined. Packets satisfying the match criteria for a class accumulate in the queue reserved for the class until they are sent, which occurs when the queue is serviced by the fair queuing process. When the maximum packet threshold you defined for the class is reached, queuing of any further packets to the class queue causes tail drop.

You use queue limits to configure Weighted Tail Drop (WTD). WTD ensures the configuration of more than one threshold per queue. Each class of service is dropped at a different threshold value to provide for QoS differentiation.

You can configure the maximum queue thresholds for the different subclasses of traffic, that is, DSCP and CoS and configure the maximum queue thresholds for each subclass.

Example

The following example configures a policy map called port-queue to contain policy for a class called dscp-1. The policy for this class is set so that the queue reserved for it has a maximum packet limit of 20 percent:

```
Device(config)# policy-map policy11
Device(config-pmap)# class dscp-1
Device(config-pmap-c)# bandwidth percent 20
Device(config-pmap-c)# queue-limit dscp 1 percent 20
```

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*

Syntax Description

cos-value	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.
percent	Specifies that the minimum and threshold values are in percentage.
min-threshold	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 CoS value.
max-threshold	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 CoS value.

Command Modes

QoS policy-map class configuration (config-pmap-c)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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

Command	Description
random-detect	Enables WRED

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-detectcos-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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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

Command	Description
random-detect cos	Specifies the CoS value of a packet, the minimum and maximum thresholds, and the maximum probability denominator used for enabling WRED.
show policy-map	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.
show policy-map interface	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.

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.

random-detect dscp *dscp-value* **percent** *min-threshold max-threshold*
no random-detect dscp *dscp-value* **percent***min-threshold max-threshold*

Syntax Description

dscp-value	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**.
percent	Specifies that the minimum and threshold values are in percentage.
min-threshold	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.
max-threshold	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.

Command Modes

QoS policy-map class configuration (config-pmap-c)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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

Command	Description
random-detect	Enables WRED

random-detect dscp-based

To base weighted random early detection (WRED) on the Differnciated Services Code Point (dscp) value of a packet, use the **random-detectdscp-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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

With the **random-detectdscp-based** command, WRED is based on the dscp value of the packet.

Use the **random-detectdscp-based** command before configuring the **random-detectdscp** 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

Command	Description
random-detect	Enables WRED.
random-detect dscp	Configures the WRED parameters for a particular DSCP value for a class policy in a policy map.

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

Syntax Description

precedence	IP precedence number. The value range is from 0 to 7; see Table 1 in the "Usage Guidelines" section.
percent	Indicates that the threshold values are in percentage.
min-threshold	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.
max-threshold	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 IP precedence.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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.

Note 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:

```
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

Command	Description
bandwidth (policy-map class)	Specifies or modifies the bandwidth allocated for a class belonging to a policy map.
random-detect dscp	Changes the minimum and maximum packet thresholds for the DSCP value.
show policy-map interface	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.
show queuing	Lists all or selected configured queuing strategies.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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

Command	Description
random-detect	Enables WRED.
random-detect precedence	Configures the WRED parameters for a particular IP precedence for a class policy in a policy map.

service-policy (Wired)

To apply a policy map to a physical port or a switch virtual interface (SVI), use the **service-policy** command in interface configuration mode. Use the **no** form of this command to remove the policy map and port association.

service-policy {**input** | **output**} *policy-map-name*
no service-policy {**input** | **output**} *policy-map-name*

Syntax Description

input *policy-map-name*	Apply the specified policy map to the input of a physical port or an SVI.
output *policy-map-name*	Apply the specified policy map to the output of a physical port or an SVI.

Command Default

No policy maps are attached to the port.

Command Modes

WLAN interface configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

A policy map is defined by the **policy map** command.

Only one policy map is supported per port, per direction. In other words, only one input policy and one output policy is allowed on any one port.

You can apply a policy map to incoming traffic on a physical port or on an SVI.

Examples

This example shows how to apply plcmap1 to an physical ingress port:

```
Device(config)# interface gigabitethernet 2/0/1
Device(config-if)# service-policy input plcmap1
```

This example shows how to remove plcmap2 from a physical port:

```
Device(config)# interface gigabitethernet 2/0/2
Device(config-if)# no service-policy input plcmap2
```

The following example displays a VLAN policer configuration. At the end of this configuration, the VLAN policy map is applied to an interface for QoS:

```
Device# configure terminal
Device(config)# class-map vlan100
Device(config-cmap)# match vlan 100
Device(config-cmap)# exit
Device(config)# policy-map vlan100
Device(config-pmap)# policy-map class vlan100
Device(config-pmap-c)# police 100000 bc conform-action transmit exceed-action drop
Device(config-pmap-c-police)# end
Device# configure terminal
```

```
Device(config)# interface gigabitethernet 1/0/5
Device(config-if)#  service-policy input vlan100
```

You can verify your settings by entering the **show running-config** privileged EXEC command.

set

To classify IP traffic by setting a Differentiated Services Code Point (DSCP) or an IP-precedence value in the packet, use the **set** command in policy-map class configuration mode. Use the **no** form of this command to remove traffic classification.

set
cos | **dscp** | **precedence** | **ip** | **qos-group**
set cos
{*cos-value* } | {**cos** | **dscp** | **precedence** | **qos-group**} [{**table** *table-map-name*}]
set dscp
{*dscp-value* } | {**cos** | **dscp** | **precedence** | **qos-group**} [{**table** *table-map-name*}]
set ip {**dscp** | **precedence**}
set precedence {*precedence-value* } | {**cos** | **dscp** | **precedence** | **qos-group**} [{**table** *table-map-name*}]
set qos-group
{*qos-group-value* | **dscp** [{**table** *table-map-name*}] | **precedence** [{**table** *table-map-name*}]}

Syntax Description

cos	Sets the Layer 2 class of service (CoS) value or user priority of an outgoing packet. You can specify these values:
	• *cos-value*—CoS value from 0 to 7. You also can enter a mnemonic name for a commonly used value.
	• Specify a packet-marking category to set the CoS value of the packet. If you also configure a table map for mapping and converting packet-marking values, this establishes the "map from" packet-marking category. Packet-marking category keywords:
	  • **cos**—Sets a value from the CoS value or user priority.
	  • **dscp**—Sets a value from packet differentiated services code point (DSCP).
	  • **precedence**—Sets a value from packet precedence.
	  • **qos-group**—Sets a value from the QoS group.
	• (Optional)**table** *table-map-name*—Indicates that the values set in a specified table map are used to set the CoS value. Enter the name of the table map used to specify the CoS value. The table map name can be a maximum of 64 alphanumeric characters.
	If you specify a packet-marking category but do not specify the table map, the default action is to copy the value associated with the packet-marking category as the CoS value. For example, if you enter the **set cos precedence** command, the precedence (packet-marking category) value is copied and used as the CoS value.

dscp	Sets the differentiated services code point (DSCP) value to mark IP(v4) and IPv6 packets. You can specify these values:
	• *cos-value*—Number that sets the DSCP value. The range is from 0 to 63. You also can enter a mnemonic name for a commonly used value.
	• Specify a packet-marking category to set the DSCP value of the packet. If you also configure a table map for mapping and converting packet-marking values, this establishes the "map from" packet-marking category. Packet-marking category keywords:
	  • **cos**—Sets a value from the CoS value or user priority.
	  • **dscp**—Sets a value from packet differentiated services code point (DSCP).
	  • **precedence**—Sets a value from packet precedence.
	  • **qos-group**—Sets a value from the QoS group.
	• (Optional)**table** *table-map-name*—Indicates that the values set in a specified table map will be used to set the DSCP value. Enter the name of the table map used to specify the DSCP value. The table map name can be a maximum of 64 alphanumeric characters.
	If you specify a packet-marking category but do not specify the table map, the default action is to copy the value associated with the packet-marking category as the DSCP value. For example, if you enter the **set dscp cos** command, the CoS value (packet-marking category) is copied and used as the DSCP value.

ip	Sets IP values to the classified traffic. You can specify these values: • **dscp**—Specify an IP DSCP value from 0 to 63 or a packet marking category. • **precedence**—Specify a precedence-bit value in the IP header; valid values are from 0 to 7 or specify a packet marking category.

precedence	Sets the precedence value in the packet header. You can specify these values:
	• *precedence-value*— Sets the precedence bit in the packet header; valid values are from 0 to 7. You also can enter a mnemonic name for a commonly used value.
	• Specify a packet marking category to set the precedence value of the packet.
	  • **cos**—Sets a value from the CoS or user priority.
	  • **dscp**—Sets a value from packet differentiated services code point (DSCP).
	  • **precedence**—Sets a value from packet precedence.
	  • **qos-group**—Sets a value from the QoS group.
	• (Optional)**table** *table-map-name*—Indicates that the values set in a specified table map will be used to set the precedence value. Enter the name of the table map used to specify the precedence value. The table map name can be a maximum of 64 alphanumeric characters.
	If you specify a packet-marking category but do not specify the table map, the default action is to copy the value associated with the packet-marking category as the precedence value. For example, if you enter the **set precedence cos** command, the CoS value (packet-marking category) is copied and used as the precedence value.

qos-group	Assigns a QoS group identifier that can be used later to classify packets. • *qos-group-value*—Sets a QoS value to the classified traffic. The range is 0 to 31. You also can enter a mnemonic name for a commonly used value. • **dscp**—Sets the original DSCP field value of the packet as the QoS group value. • **precedence**—Sets the original precedence field value of the packet as the QoS group value. • (Optional)**table** *table-map-name*—Indicates that the values set in a specified table map will be used to set the DSCP or precedence value. Enter the name of the table map used to specify the value. The table map name can be a maximum of 64 alphanumeric characters. If you specify a packet-marking category (**dscp** or **precedence**) but do not specify the table map, the default action is to copy the value associated with the packet-marking category as the QoS group value. For example, if you enter the **set qos-group precedence** command, the precedence value (packet-marking category) is copied and used as the QoS group value.

Command Default

No traffic classification is defined.

Command Modes

Policy-map class configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was intro

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 [*interface-id*]	(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 Fuji 16.9.2	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
Gigabitethernet 2/0/4
auto qos voip cisco-softphone

Gigabitethernet 2/0/5
auto qos voip cisco-phone


Gigabitethernet 2/0/6
auto qos voip cisco-phone
```

This is an example of output from the **show auto qos interface** *interface-id* command when the **auto qos voip cisco-phone** interface configuration command is entered:

```
Device# show auto qos interface Gigabitethernet 2/0/5
Gigabitethernet 2/0/5
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 Gigabitethernet 3/0/1
```

```
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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Examples

This is an example of output from the **show class-map** command:

```
Device# show class-map
 Class Map match-any videowizard_10-10-10-10 (id 2)
   Match access-group name videowizard_10-10-10-10

 Class Map match-any class-default (id 0)
   Match any
 Class Map match-any dscp5 (id 3)
   Match ip dscp 5
```

show platform hardware fed switch

To display device-specific hardware information, use the **show platform hardware fed switch***switch_number* command.

This topic elaborates only the QoS-specific options, that is, the options available with the **show platform hardware fed switch** {*switch_num* | **active** | **standby** } **qos** command.

show platform hardware fed switch {*switch_num* | **active** | **standby**} **qos** {**afd** | {**config type** *type* | [{**asic** *asic_num*}] | **stats clients** {**all** | **bssid** *id* | **wlanid** *id* }} | **dscp-cos counters** {**iifd_id** *id* | **interface***type number*} | **le-info** | {**iifd_id** *id* | **interface** *type number*} | **policer config** {**iifd_id** *id* | **interface** *type number*} | **queue** | {**config** | {**iifd_id** *id* | **interface** *type number* | **internal port-type** *type* {**asic** *number* [{**port_num**}]}} | **label2qmap** | [{**aqmrepqostbl** | **iqslabeltable** | **sqslabeltable**}] | {**asic***number*} | **stats** | {**iifd_id** *id* | **interface** *type number* | **internal** {**cpu policer** | **port-type** *type* **asic** *number*} {**asic***number* [{**port_num**}]}}} | **resource**}

Syntax Description

switch {*switch_num* | **active** | **standby** }	Switch for which you want to display information. You have the following options: • *switch_num*—ID of the switch. • **active**—Displays information relating to the active switch. • **standby**—Displays information relating to the standby switch, if available.
qos	Displays QoS hardware information. You must choose from the following options: • **afd** —Displays Approximate Fair Drop (AFD) information in hardware. • **dscp-cos**—Displays information dscp-cos counters for each port. • **leinfo**—Displays logical entity information. • **policer**—Displays QoS policer information in hardware. • **queue**—Displays queue information in hardware. • **resource**—Displays hardware resource information.
afd {**config type** | **stats client** }	You must choose from the options under **config type** or **stats client** : **config type**: • **client**—Displays wireless client information • **port**—Displays port-specific information • **radio**—Displays wireless radio information • **ssid**—Displays wireless SSID information **stats client** : • **all**—Displays statistics of all client. • **bssid**—Valid range is from 1 to 4294967295. • **wlanid**—Valid range is from to 1 4294967295

asic*asic_num*	(Optional) ASIC number. Valid range is from 0 to 255.
dscp-cos counters { **iifd_id** *id* | **interface** *type number* }	Displays per port dscp-cos counters. You must choose from the following options under **dscp-cos counters**: • **iif_id** *id*—The target interface ID. Valid range is from 1 to 4294967295. • **interface** *type number*—Target interface type and ID.
leinfo	You must choose from the following options under **dscp-cos counters**: • **iif_id** *id*—The target interface ID. Valid range is from 1 to 4294967295. • **interface** *type number*—Target interface type and ID.
policer config	Displays configuration information related to policers in hardware. You must choose from the following options: • **iif_id** *id*—The target interface ID. Valid range is from 1 to 4294967295. • **interface** *type number*—Target interface type and ID.
queue {**config** {**iif_id** *id* | **interface** *type number* | **internal**} | **label2qmap** | **stats**}	Displays queue information in hardware. You must choose from the following options: • **config**—Configuration information. You must choose from the following options: • **iif_id** *id*—The target interface ID. Valid range is from 1 to 4294967295. • **interface** *type number*—Target interface type and ID. • **internal**—Displays internal queue related information. • **label2qmap**—Displays hardware label to queue mapping information. You can choose from the following options: • (Optional) **aqmrepqostbl**— AQM REP QoS label table lookup. • (Optional) **iqslabeltable**—IQS QoS label table lookup. • (Optional) **sqslabeltable**—SQS and local QoS label table lookup. • **stats**—Displays queue statistics. You must choose from the following options: • **iif_id** *id*—The target interface ID. Valid range is from 1 to 4294967295. • **interface** *type number*—Target interface type and ID. • **internal** {**cpu policer** | **port_type** *port_type* **asic** *asic_num* [**port_num** *port_num*] }—Displays internal queue related information.
resource	Displays hardware resource usage information. You must enter the following keyword: **usage**

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

This is an example of output from the**show platform hardware fed switch***switch_number***qos queue stats internal cpu policer** command

```
Device#show platform hardware fed switch 3 qos queue stats internal cpu policer

                                                  (default)   (set)
QId PlcIdx  Queue Name                 Enabled     Rate      Rate       Drop
-----------------------------------------------------------------------------
0    11     DOT1X Auth                  No        1000       1000          0
1    1      L2 Control                  No        500        500           0
2    14     Forus traffic               No        1000       1000          0
3    0      ICMP GEN                    Yes       200        200           0
4    2      Routing Control             Yes       1800       1800          0
5    14     Forus Address resolution    No        1000       1000          0
6    3      ICMP Redirect               No        500        500           0
7    6      WLESS PRI-5                 No        1000       1000          0
8    4      WLESS PRI-1                 No        1000       1000          0
9    5      WLESS PRI-2                 No        1000       1000          0
10   6      WLESS PRI-3                 No        1000       1000          0
11   6      WLESS PRI-4                 No        1000       1000          0
12   0      BROADCAST                   Yes       200        200           0
13   10     Learning cache ovfl         Yes       100        100           0
14   13     Sw forwarding               Yes       1000       1000          0
15   8      Topology Control            No        13000      13000         0
16   12     Proto Snooping              No        500        500           0
17   16     DHCP Snooping               No        1000       1000          0
18   9      Transit Traffic             Yes       500        500           0
19   10     RPF Failed                  Yes       100        100           0
20   15     MCAST END STATION           Yes       2000       2000          0
21   13     LOGGING                     Yes       1000       1000          0
22   7      Punt Webauth                No        1000       1000          0
23   10     Crypto Control              Yes       100        100           0
24   10     Exception                   Yes       100        100           0
25   3      General Punt                No        500        500           0
26   10     NFL SAMPLED DATA            Yes       100        100           0
27   2      SGT Cache Full              Yes       1800       1800          0
28   10     EGR Exception               Yes       100        100           0
29   16     Show frwd                   No        1000       1000          0
30   9      MCAST Data                  Yes       500        500           0
31   10     Gold Pkt                    Yes       100        100           0
```

show platform software fed switch qos

To display device-specific software information, use the **show platform hardware fed switch** *switch_number* command.

This topic elaborates only the QoS-specific options available with the **show platform software fed switch** {*switch_num* | **active** | **standby** } **qos** command.

show platform software fed switch{*switch number* | **active** | **standby** }**qos**{**avc** | **internal** | **label2qmap** | **nflqos** | **policer** | **policy** | **qsb** | **tablemap**}

Syntax Description

switch {*switch_num* | **active** | **standby** }	The device for which you want to display information. • *switch_num*—Enter the switch ID. Displays information for the specified switch. • **active**—Displays information for the active switch. • **standby**—Displays information for the standby switch, if available.
qos	Displays QoS software information. Choose one the following options: • **avc** : Displays Application Visibility and Control (AVC) QoS information. • **internal**: Displays internal queue-related information. • **label2qmap**: Displays label to queue map table information. • **nflqos**: Displays NetFlow QoS information. • **policer**: Displays QoS policer information in hardware. • **policy**: Displays QoS policy information. • **qsb**: Displays QoS sub-block information. • **tablemap**: Displays table mapping information for QoS egress and ingress queues.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

show platform software fed switch qos qsb

To display QoS sub-block information, use the **show platform software fed switch** *switch_number* **qos qsb** command.

show platform software fed switch{*switch number* | **active** | **standby**}**qosqsb**{**brief** | [{**all** | **type** | {**client***client_id* | **port** *port_number* | **radio***radio_type* | **ssid***ssid*}}] | **iif_id***id* | **interface** | {**Auto-Template***interface_number* | **BDI***interface_number* | **Capwap***interface_number* | **GigabitEthernet***interface_number* | **InternalInterface***interface_number* | **Loopback***interface_number* | **Null***interface_number* | **Port-channel***interface_number* | **TenGigabitEthernet***interface_number* | **Tunnel***interface_number* | **Vlan***interface_number*}}

Syntax Description

switch {*switch_num* | **active** | **standby** }	The switch for which you want to display information. • *switch_num*—Enter the ID of the switch. Displays information for the specified switch. • **active**—Displays information for the active switch. • **standby**—Displays information for the standby switch, if available.
qos qsb	Displays QoS sub-block software information.

qsb {**brief** | **iif_id** | **interface**}	**brief** • **all**—Displays information for all client. • **type**—Displays qsb information for the specified target type: • **client**—Displays QoS qsb information for wireless clients • **port**—Displays port-specific information • **radio**—Displays QoS qsb information for wireless radios • **ssid**—Displays QoS qsb information for wireless networks **iif_id**—Displays information for the iif_ID **interface**—Displays QoS qsb information for the specified interface: • **Auto-Template**—Auto-template interface between 1 and 999. • **BDI**—Bridge-domain interface between 1 and 16000. • **Capwap**—CAPWAP interface between 0 and 2147483647. • **GigabitEthernet**—GigabitEthernet interface between 0 and 9. • **InternalInterface**—Internal interface between 0 and 9. • **Loopback**—Loopback interface between 0 and 2147483647. • **Null**—Null interface 0-0 • **Port-Channel**—Port-channel interface between 1 and 128. • **TenGigabitEthernet**—TenGigabitEthernet interface between 0 and 9. • **Tunnel**—Tunnel interface between 0 and 2147483647. • **Vlan**—VLAN interface between 1 and 4094.

Command Modes

User EXEC

Privileged EXEC

Command History

This command was introduced.

This is an example of the output for the**show platform software fed switch***switch_number***qos qsb** command

```
Device#sh pl so fed sw 3 qos qsb interface g3/0/2

  QoS subblock information:
  Name:GigabitEthernet3/0/2 iif_id:0x0000000000007b iif_type:ETHER(146)
  qsb ptr:0xffd8573350
  Port type = Wired port
  asic_num:0 is_uplink:false init_done:true
  FRU events: Active-0, Inactive-0
  def_qos_label:0 def_le_priority:13
  trust_enabled:false trust_type:TRUST_DSCP ifm_trust_type:1
```

```
 LE priority:13 LE trans_index(in, out): (0,0)
 Stats (plc,q) export counters (in/out): 0/0
 Policy Info:
   Ingress Policy: pmap::{(0xffd8685180,AutoQos-4.0-CiscoPhone-Input-Policy,1083231504,)}
    tcg::{0xffd867ad10,GigabitEthernet3/0/2 tgt(0x7b,IN) level:0 num_tccg:4 num_child:0},
status:VALID,SET_INHW
   Egress Policy: pmap::{(0xffd86857d0,AutoQos-4.0-Output-Policy,1076629088,)}
    tcg::{0xffd8685b40,GigabitEthernet3/0/2 tgt(0x7b,OUT) level:0 num_tccg:8 num_child:0},
status:VALID,SET_INHW
   TCG(in,out):(0xffd867ad10, 0xffd8685b40) le_label_id(in,out):(2, 1)
 Policer Info:
   num_ag_policers(in,out)[1r2c,2r3c]: ([0,0],[0,0])
   num_mf_policers(in,out): (0,0)
   num_afd_policers:0
   [ag_plc_handle(in,out) = (0xd8688220,0)]
   [mf_plc_handle(in,out)=((nil),(nil)) num_mf_policers:(0,0)
     base:(0xffffffff,0xffffffff) rc:(0,0)]
 Queueing Info:
   def_queuing = 0, shape_rate:0 interface_rate_kbps:1000000
   Port shaper:false
   lbl_to_qmap_index:1
   Physical qparams:
    Queue Config: NodeType:Physical Id:0x40000049 parent:0x40000049 qid:0 attr:0x1 defq:0

       PARAMS: Excess Ratio:1 Min Cir:1000000 QBuffer:0
       Queue Limit Type:Single Unit:Percent Queue Limit:44192
       SHARED Queue
```

show policy-map

To display quality of service (QoS) policy maps, which define classification criteria for incoming traffic, use the **show policy-map** command in EXEC mode.

show policy-map [{*policy-map-name* | **interface** *interface-id*}]

show policy-map interface {**Auto-template** | **Capwap** | **GigabitEthernet** | **GroupVI** | **InternalInterface** | **Loopback** | **Lspvif** | **Null** | **Port-channel** | **TenGigabitEthernet** | **Tunnel** | **Vlan** | **brief** | **class** | **input** | **output**}

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	Modification
Cisco IOS XE Fuji 16.9.2	This command w

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 gigabitethernet 1/0/48

  Service-policy output: port_shape_parent

    Class-map: class-default (match-any)
      191509734 packets
      Match: any
      Queueing

      (total drops) 524940551420
      (bytes output) 14937264500
      shape (average) cir 250000000, bc 2500000, be 2500000
      target shape rate 250000000

      Service-policy : child_trip_play

        queue stats for all priority classes:
          Queueing
          priority level 1
```

```
  (total drops) 524940551420
  (bytes output) 14937180648

queue stats for all priority classes:
  Queueing
  priority level 2

  (total drops) 0
  (bytes output) 0

Class-map: dscp56 (match-any)
  191508445 packets
  Match:  dscp cs7 (56)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Priority: Strict,

  Priority Level: 1
  police:
      cir 10 %
      cir 25000000 bps, bc 781250 bytes
    conformed 0 bytes; actions: >>>>>counters not supported
      transmit
    exceeded 0 bytes; actions:
      drop
    conformed 0000 bps, exceeded 0000 bps  >>>>>counters not supported
```

show 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

switch *switch-number*	(Optional) Displays QoS-related information for a specific switch.
active	(Optional) Displays QoS-related information for the active instance of the switch.
all	(Optional) Displays QoS-related information for all instances of the switch.
standby	(Optional) Displays QoS-related information for the standby instance of the switch.
control-plane	(Optional) Displays QoS-related information for the control-plane.
interface *interface-name*	(Optional) Displays QoS-related information for a specified interface.
all	(Optional) Displays QoS-related information for all interfaces.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

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
.
.
```

```
.
------------------ show platform software fed switch 1 qos policy target brief
------------------


TCG summary for policy: system-cpp-policy

Loc Interface              IIF-ID           Dir tccg Child #m/p/q  State:(cfg,opr)
--- ---------------------- ---------------- --- ---- ----- ------- ---------------
?:255 Control Plane      0x00000001000001 OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4da31c8
?:0 CoPP-Queue-0         0x0000000100000d OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4da41e8
?:0 CoPP-Queue-1         0x0000000100000e OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4dbede8
?:0 CoPP-Queue-2         0x0000000100000f OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4dc2df8
?:0 CoPP-Queue-3         0x00000001000010 OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4dc6e08
?:0 CoPP-Queue-4         0x00000001000011 OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4dcae18
?:0 CoPP-Queue-5         0x00000001000012 OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4dcee28
?:0 CoPP-Queue-6         0x00000001000013 OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4dd2e38
?:0 CoPP-Queue-7         0x00000001000014 OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4dd6e48
?:0 CoPP-Queue-8         0x00000001000015 OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4ddae58
?:0 CoPP-Queue-9         0x00000001000016 OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4ddee68
?:0 CoPP-Queue-10        0x00000001000017 OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4de2e78
?:0 CoPP-Queue-11        0x00000001000018 OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4de6e88
?:0 CoPP-Queue-12        0x00000001000019 OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4deae98
?:0 CoPP-Queue-13        0x0000000100001a OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4deeea8
?:0 CoPP-Queue-14        0x0000000100001b OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4df2eb8
?:0 CoPP-Queue-15        0x0000000100001c OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4df6ec8
?:0 CoPP-Queue-16        0x0000000100001d OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4dfaed8
?:0 CoPP-Queue-17        0x0000000100001e OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4dfeee8
?:0 CoPP-Queue-18        0x0000000100001f OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4e02ef8
?:0 CoPP-Queue-19        0x00000001000020 OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4e06f08
?:0 CoPP-Queue-20        0x00000001000021 OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4e0ae88
?:0 CoPP-Queue-21        0x00000001000022 OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4e0ee98
?:0 CoPP-Queue-22        0x00000001000023 OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4e12ea8
?:0 CoPP-Queue-23        0x00000001000024 OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4e16eb8
?:0 CoPP-Queue-24        0x00000001000025 OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4e1aec8
?:0 CoPP-Queue-25        0x00000001000026 OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4e1eed8
?:0 CoPP-Queue-26        0x00000001000027 OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4e22ee8
?:0 CoPP-Queue-27        0x00000001000028 OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4e26ef8
?:0 CoPP-Queue-28        0x00000001000029 OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4e2af08
?:0 CoPP-Queue-29        0x0000000100002a OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4e2ef18
?:0 CoPP-Queue-30        0x0000000100002b OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4e32f28
?:0 CoPP-Queue-31        0x0000000100002c OUT   22     0 0/17/0  VALID,SET_INHW  0xffe4e36f38

------------------ show platform software fed switch 1 qos policy summary ------------------


Policymap Summary: (counters)
  CGID     Clases 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**}

Syntax Description

cisco-phone	Configures a Cisco IP phone
cts	Configures a Cisco TelePresence System
ip-camera	Configures an IP Video Surveillance Camera (IPVSC)
media-player	Configures a Cisco Digital Media Player (DMP)

Command Default

Trust disabled

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Use the **trust device** command on the following types of interfaces:

- **Auto**— auto-template interface
- **Capwap**—CAPWAP tunnel interface
- **GigabitEthernet**—Gigabit Ethernet IEEE 802
- **GroupVI**—Group virtual interface
- **Internal Interface**—Internal interface
- **Loopback**—Loopback interface
- **Null**—Null interface
- **Port-channel**—Ethernet Channel interface
- **TenGigabitEthernet--**10-Gigabit Ethernet
- **Tunnel**—Tunnel interface
- **Vlan**—Catalyst VLANs
- **range**—**interface range** command

Example

The following example configures trust for a Cisco IP phone in Interface GigabitEthernet 1/0/1:

```
Device(config)# interface gigabitethernet 1/0/1
Device(config-if)# trust device cisco-phone
```

PART IX

Routing

- IP Routing Commands, on page 1063

IP Routing Commands

- accept-lifetime, on page 1065
- address-family ipv6 (OSPF), on page 1068
- area nssa, on page 1069
- area virtual-link, on page 1071
- authentication (BFD), on page 1074
- bfd, on page 1075
- bfd all-interfaces, on page 1077
- bfd check-ctrl-plane-failure, on page 1078
- bfd echo, on page 1079
- bfd slow-timers, on page 1081
- bfd template, on page 1083
- bfd-template single-hop, on page 1084
- default-information originate (OSPF), on page 1085
- distance (OSPF), on page 1087
- eigrp log-neighbor-changes, on page 1090
- eigrp log-neighbor-warnings, on page 1092
- ip authentication key-chain eigrp, on page 1094
- ip authentication mode eigrp, on page 1095
- ip bandwidth-percent eigrp, on page 1096
- ip cef load-sharing algorithm, on page 1097
- ip prefix-list, on page 1098
- ip hello-interval eigrp, on page 1101
- ip hold-time eigrp, on page 1102
- ip load-sharing, on page 1103
- ip ospf database-filter all out, on page 1104
- ip ospf name-lookup, on page 1105
- ip split-horizon eigrp, on page 1106
- ip summary-address eigrp, on page 1107
- ip route static bfd, on page 1109
- ipv6 route static bfd, on page 1111
- metric weights (EIGRP), on page 1112
- neighbor description, on page 1114
- network (EIGRP), on page 1115

- nsf (EIGRP), on page 1117
- offset-list (EIGRP), on page 1119
- redistribute (IP), on page 1121
- redistribute (IPv6), on page 1129
- redistribute maximum-prefix (OSPF), on page 1132
- route-map, on page 1134
- router-id, on page 1137
- router eigrp, on page 1138
- router ospfv3, on page 1139
- send-lifetime, on page 1140
- show ip eigrp interfaces, on page 1143
- show ip eigrp neighbors, on page 1146
- show ip eigrp topology, on page 1149
- show ip eigrp traffic, on page 1154
- show ip ospf, on page 1156
- show ip ospf border-routers, on page 1164
- show ip ospf database, on page 1165
- show ip ospf interface, on page 1174
- show ip ospf neighbor, on page 1177
- show ip ospf virtual-links, on page 1183
- summary-address (OSPF), on page 1184
- timers throttle spf, on page 1186

accept-lifetime

To set the time period during which the authentication key on a key chain is received as valid, use the **accept-lifetime** command in key chain key configuration mode. To revert to the default value, use the **no** form of this command.

accept-lifetime [**local**] *start-time* { **infinite** *end-time* | **duration** *seconds* }
no accept-lifetime

Syntax Description

local	Specifies the time in local timezone.
start-time	Beginning time that the key specified by the **key** command is valid to be received. The syntax can be either of the following: *hh* **:** *mm* **:** *ss month date year* *hh* **:** *mm* **:** *ss date month year* • *hh*: Hours • *mm*: Minutes • *ss*: Seconds • *month*: First three letters of the month • *date*: Date (1-31) • *year*: Year (four digits) The default start time and the earliest acceptable date is January 1, 1993.
infinite	Key is valid to be received from the *start-time* value on.
end-time	Key is valid to be received from the *start-time* value until the *end-time*value. The syntax is the same as that for the *start-time*value. The *end-time* value must be after the *start-time*value. The default end time is an infinite time period.
duration *seconds*	Length of time (in seconds) that the key is valid to be received. The range is from 1 to 864000.

Command Default

The authentication key on a key chain is received as valid forever (the starting time is January 1, 1993, and the ending time is infinite).

Command Modes

Key chain key configuration (config-keychain-key)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Only DRP Agent, Enhanced Interior Gateway Routing Protocol (EIGRP), and Routing Information Protocol (RIP) Version 2 use key chains.

Specify a *start-time* value and one of the following values: **infinite**, *end-time*, or **duration** *seconds*.

We recommend running Network Time Protocol (NTP) or some other time synchronization method if you assign a lifetime to a 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.

Examples

The following example configures a key chain named chain1. The key named key1 will be accepted from 1:30 p.m. to 3:30 p.m. and will be sent from 2:00 p.m. to 3:00 p.m. The key named key2 will be accepted from 2:30 p.m. to 4:30 p.m. and will be sent from 3:00 p.m. to 4:00 p.m. The overlap allows for migration of keys or a discrepancy in the set time of the router. There is a 30-minute leeway on each side to handle time differences.

```
Device(config)# interface GigabitEthernet1/0/1
Device(config-if)# ip rip authentication key-chain chain1
Device(config-if)# ip rip authentication mode md5
Device(config-if)# exit
Device(config)# router rip
Device(config-router)# network 172.19.0.0
Device(config-router)# version 2
Device(config-router)# exit
Device(config)# key chain chain1
Device(config-keychain)# key 1
Device(config-keychain-key)# key-string key1
Device(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 1996 duration 7200
Device(config-keychain-key)# send-lifetime 14:00:00 Jan 25 1996 duration 3600
Device(config-keychain-key)# exit
Device(config-keychain)# key 2
Device(config-keychain)# key-string key2
Device(config-keychain)# accept-lifetime 14:30:00 Jan 25 1996 duration 7200
Device(config-keychain)# send-lifetime 15:00:00 Jan 25 1996 duration 3600
```

The following example configures a key chain named chain1 for EIGRP address-family. The key named key1 will be accepted from 1:30 p.m. to 3:30 p.m. and be sent from 2:00 p.m. to 3:00 p.m. The key named key2 will be accepted from 2:30 p.m. to 4:30 p.m. and be sent from 3:00 p.m. to 4:00 p.m. The overlap allows for migration of keys or a discrepancy in the set time of the router. There is a 30-minute leeway on each side to handle time differences.

```
Device(config)# router eigrp 10
Device(config-router)# address-family ipv4 autonomous-system 4453
Device(config-router-af)# network 10.0.0.0
Device(config-router-af)# af-interface ethernet0/0
Device(config-router-af-interface)# authentication key-chain trees
Device(config-router-af-interface)# authentication mode md5
Device(config-router-af-interface)# exit
Device(config-router-af)# exit
Device(config-router)# exit
Device(config)# key chain chain1
Device(config-keychain)# key 1
Device(config-keychain-key)# key-string key1
Device(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 1996 duration 7200
Device(config-keychain-key)# send-lifetime 14:00:00 Jan 25 1996 duration 3600
Device(config-keychain-key)# exit
Device(config-keychain)# key 2
Device(config-keychain-key)# key-string key2
Device(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 1996 duration 7200
Device(config-keychain-key)# send-lifetime 15:00:00 Jan 25 1996 duration 3600
```

Related Commands

Command	Description
key	Identifies an authentication key on a key chain.
key chain	Defines an authentication key-chain needed to enable authentication for routing protocols.
key-string (authentication)	Specifies the authentication string for a key.
send-lifetime	Sets the time period during which an authentication key on a key chain is valid to be sent.
show key chain	Displays authentication key information.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command w

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

Command	Description
router ospfv3	Enters OSPFv3 router configuration mode.

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 commandarea *area-id* **nssa** [**no-redistribution**] [**default-information-originate** [**metric**] [**metric-type**]] [**no-summary**] [**nssa-only**]
no area *area-id* **nssa** [**no-redistribution**] [**default-information-originate** [**metric**] [**metric-type**]] [**no-summary**] [**nssa-only**]

Syntax Description

area-id	Identifier for the stub area or NSSA. The identifier can be specified as either a decimal value or an IP address.
no-redistribution	(Optional) Used when the router is an NSSA Area Border Router (ABR) and you want the **redistribute** command to import routes only into the normal areas, but not into the NSSA area.
default-information-originate	(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).
metric	(Optional) Specifies the OSPF default metric.
metric-type	(Optional) Specifies the OSPF metric type for default routes.
no-summary	(Optional) Allows an area to be an NSSA but not have summary routes injected into it.
nssa-only	(Optional) Limits the default advertisement to this NSSA area by setting the propagate (P) bit in the type-7 LSA to zero.

Command Default

No NSSA area is defined.

Command Modes

Router address family topology configuration (config-router-af-topology) Router configuration (config-router)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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
```

Related Commands

Command	Description
redistribute	Redistributes routes from one routing domain into another routing domain.

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 111:

area-id	Area ID assigned to the virtual link. This can be either a decimal value or a valid IPv6 prefix. There is no default.
router-id	Router ID associated with the virtual link neighbor. The router ID appears in the **show ip ospf** or **show ipv6 display** command. There is no default.
authentication	Enables virtual link authentication.
key-chain	Configures a key-chain for cryptographic authentication keys.
chain-name	Name of the authentication key that is valid.
hello-interval *seconds*	(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.
retransmit-interval *seconds*	(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.
transmit-delay *seconds*	(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.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
Device(config)# ipv6 router ospf 1
Device(config)# log-adjacency-changes
Device(config)# area 1 virtual-link 192.168.255.1
```

The following example establishes a virtual link in OSPF for IPv6:

```
Device(config)# ipv6 router ospf 1
Device(config)# log-adjacency-changes
Device(config)# 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:

```
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:

```
Device(config)# area 1 virtual-link 192.168.255.1 authentication key-chain ospf-chain-1
```

Related Commands

Command	Description
area	Configures OSPFv3 area parameters.
show ip ospf	Enables the display of general information about OSPF routing processes.
show ipv6 ospf	Enables the display of general information about OSPF routing processes.
ttl-security hops	Enables checking of TTL values on OSPF packets from neighbors or setting TTL values sent to neighbors.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

You can configure authentication in single hop templates. We recommend that you configure authentication to enhance security. Authentication must be configured on each BFD source-destination pair, and authentication parameters must match on both devices.

Examples

The following example shows how to configure authentication for the template1 BFD single-hop template:

```
Device>enable
Device#configuration terminal
Device(config)#bfd-template single-hop template1
Device(config-bfd)#authentication sha-1 keychain bfd-singlehop
```

bfd

To set the baseline Bidirectional Forwarding Detection (BFD) session parameters on an interface, use the **bfd** interface configuration mode. To remove the baseline BFD session parameters, use the **no** form of this command

bfd interval *milliseconds* **min_rx** *milliseconds* **multiplier** *multiplier-value*
no bfd interval *milliseconds* **min_rx** *milliseconds* **multiplier** *multiplier-value*

Syntax Description

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-valueargument is from 3 to 50.

Command Default

No baseline BFD session parameters are set.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The bfd command can be configured on SVI, Ethernet and port-channel interfaces.

If BFD runs on a port channel interface, BFD has a timer value restriction of 750 * 3 milliseconds.

The bfd interval configuration is not removed when:

- an IPv4 address is removed from an interface
- an IPv6 address is removed from an interface
- IPv6 is disabled from an interface
- an interface is shutdown
- IPv4 CEF is disabled globally or locally on an interface
- IPv6 CEF is disabled globally or locally on an interface

The bfd interval configuration is removed when the subinterface on which its is configured is removed.

Note If we configure bfd interval command in interface config mode, then bfd echo mode is enabled by default. We need to enable either no ip redirect (if BFD echo is needed) or no bfd echo in interface config mode.

Before using BFD echo mode, you must disable sending Internet Control Message Protocol (ICMP) redirect messages by entering the no ip redirect command, in order to avoid high CPU utilization.

Examples

The following example shows the BFD session parameters set for Gigabit Ethernet 1/0/3:

```
Device>enable
Device#configuration terminal
Device(config)#interface gigabitethernet 1/0/3
Device(config-if)#bfd interval 100 min_rx 100 multiplier 3
```

bfd all-interfaces

To enable Bidirectional Forwarding Detection (BFD) for all interfaces participating in the routing process, use the **bfd all-interfaces** command in router configuration or address family interface configuration mode. To disable BFD for all neighbors on a single interface, use the **no** form of this command

bfd all-interfaces
no bfd all-interfaces

Syntax Description

This command has no arguments or keywords.

Command Default

BFD is disabled on the interfaces participating in the routing process.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

To enable BFD for all interfaces, enter the bfd all-interfaces command in router configuration mode

Examples

The following example shows how to enable BFD for all Enhanced Interior Gateway Routing Protocol (EIGRP) neighbors:

```
Device>enable
Device#configuration terminal
Device(config)#router eigrp 123
Device(config-router)#bfd all-interfaces
Device(config-router)#end
```

The following example shows how to enable BFD for all Intermediate System-to-Intermediate System (IS-IS) neighbors:

```
Device> enable
Device#configuration terminal
Device(config)#router isis tag1
Device(config-router)#bfd all-interfaces
Device(config-router)#end
```

bfd check-ctrl-plane-failure

To enable Bidirectional Forwarding Detection (BFD) control plane failure checking for the Intermediate System-to-Intermediate System (IS-IS) routing protocol, use the **bfd check-control-plane-failure** command in router configuration mode. To disable control plane failure detection, use the **no** form of this command

bfd check-ctrl-plane-failure
no bfd check-ctrl-plane-failure

Syntax Description

This command has no arguments or keywords.

Command Default

BFD control plane failure checking is disabled.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The bfd check-ctrl-plane-failure command can be configured for an IS-IS routing process only. The command is not supported on other protocols.

When a switch restarts, a false BFD session failure can occur, where neighboring routers behave as if a true forwarding failure has occurred. However, if the bfd check-ctrl-plane-failure command is enabled on a switch, the router can ignore control plane related BFD session failures. We recommend that you add this command to the configuration of all neighboring routers just prior to a planned router restart, and that you remove the command from all neighboring routers when the restart is complete.

Examples

The following example enables BFD control plane failure checking for the IS-IS routing protocol:

```
Device>enable
Device#configuration terminal
Device(config)#router isis
Device(config-router)#bfd check-ctrl-plane-failure
Device(config-router)#end
```

bfd echo

To enable Bidirectional Forwarding Detection (BFD) echo mode, use the **bfd echo** command in interface configuration mode. To disable BFD echo mode, use the **no** form of this command

bfd echo
no bfd echo

Syntax Description

This command has no arguments or keywords.

Command Default

BFD echo mode is enabled by default if BFD is configured using bfd interval command in interface configuration mode.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Examples

The following example shows how to configure the BFD slow timers value to 14,000 milliseconds:

```
Device(config)#bfd slow-timers 14000
```

The following output from the show bfd neighbors details command shows that the BFD slow timers value of 14,000 milliseconds has been implemented. The values for the MinTxInt and MinRxInt will correspond to the configured value for the BFD slow timers. The relevant command output is shown in bold.

```
Device#show bfd neighbors details
OurAddr      NeighAddr   LD/RD  RH/RS  Holdown(mult) State Int
172.16.1.2   172.16.1.1  1/6    Up     0 (3 )        Up    Fa0/1
Session state is UP and using echo function with 100 ms interval.
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 14000, MinRxInt: 14000, Multiplier: 3
Received MinRxInt: 1000000, Received Multiplier: 3
Holdown (hits): 3600(0), Hello (hits): 1200(337)
Rx Count: 341, Rx Interval (ms) min/max/avg: 1/1008/882 last: 364 ms ago
Tx Count: 339, Tx Interval (ms) min/max/avg: 1/1016/886 last: 632 ms ago
Registered protocols: EIGRP
Uptime: 00:05:00
Last packet: Version: 1            - Diagnostic: 0
             State bit: Up         - Demand bit: 0
             Poll bit: 0           - Final bit: 0
             Multiplier: 3         - Length: 24
             My Discr.: 6          - Your Discr.: 1
             Min tx interval: 1000000   - Min rx interval: 1000000
             Min Echo interval: 50000
```

Note

- If the BFD session is down, then the BFD control packets will be sent with the slow timer interval.
- If the BFD session is up, then if echo is enabled, then BFD control packets will be sent in negotiated slow timer interval and echo packets will be sent in negotiated configured BFD interval. If echo is not enabled, then BFD control packets will be sent in negotiated configured interval.

bfd template

To 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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Even if you have not created the template by using the **bfd-template** command, you can configure the name of the template under an interface, but the template is considered invalid until you define the template. You do not have to reconfigure the template name again. It becomes valid automatically.

Examples

```
Device> enable
Device#configuration terminal
Device(config)#interface Gigabitethernet 1/3/0
Device(config-if)#bfd template template1
```

bfd-template single-hop

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The bfd-template command allows you to create a BFD template and places the device in BFD configuration mode. The template can be used to specify a set of BFD interval values. BFD interval values specified as part of the BFD template are not specific to a single interface.

Examples

The following example shows how to create a BFD template and specify BFD interval values:

```
Device>enable
Device#configuration terminal
Device(config)#bfd-template single-hop node1
Device(bfd-config)#interval min-tx 100 min-rx 100 multiplier 3
Device(bfd-config)#echo
```

The following example shows how to create a BFD single-hop template and configure BFD interval values and an authentication key chain:

```
Device> enable
Device#configuration terminal
Device(config)#bfd-template single-hop template1
Device(bfd-config)#interval min-tx 200 min-rx 200 multiplier 3
Device(bfd-config)#authentication keyed-sha-1 keychain bfd_singlehop
```

Note BFD echo is not enabled by default in the bfd-template configuration. This needs to configured explicitly.

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 Fuji 16.9.2	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

Command	Description
default-information	Accepts exterior or default information into Enhanced Interior Gateway Routing Protocol (EIGRP) processes.
default-metric	Sets default metric values for routes.
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.

distance (OSPF)

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

weight	Administrative distance. Range is 10 to 255. Used alone, the *weight* 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.
ip-address	(Optional) IP address in four-part dotted-decimal notation.
wildcard-mask	(Optional) Wildcard mask in four-part, dotted-decimal format. A bit set to 1 in the *wildcard-mask* argument instructs the software to ignore the corresponding bit in the address value.
access-list-name	(Optional) Name of an IP access list to be applied to incoming routing updates.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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 112: Default Administrative Distances

Rate Source	Default Distance
Connected interface	0
Static route out on interface	0
Static route to next hop	1
EIGRP summary route	5
External BGP	20
Internal EIGRP	90
OSPF	110
IS-IS	115
RIP version 1 and 2	120
External EIGRP	170
Internal BGP	200
Unknown	255

Task ID

Task ID	Operations
ospf	read, write

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

Command	Description
distance bgp	Allows the use of external, internal, and local administrative distances that could be a better route to a BGP node.
distance ospf	Allows the use of external, internal, and local administrative distances that could be a better route to an OSPF node.

Command	Description
router ospf	Configures the OSPF routing process.

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 thiscommand.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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
```

Related Commands

Command	Description
address-family (EIGRP)	Enters address-family configuration mode to configure an EIGRP routing instance.
exit-address-family	Exits address-family configuration mode.
exit-service-family	Exits service-family configuration mode.
router eigrp	Configures the EIGRP routing process.
service-family	Specifies service-family configuration mode.

eigrp log-neighbor-warnings

To enable the logging of Enhanced Interior Gateway Routing Protocol (EIGRP) neighbor warning messages, use the **eigrp log-neighbor-warnings** command in router configuration mode, address-family configuration mode, or service-family configuration mode. To disable the logging of EIGRP neighbor warning messages, use the **no** form of this command.

eigrp log-neighbor-warnings [*seconds*]
no eigrp log-neighbor-warnings

Syntax Description

seconds	(Optional) The time interval (in seconds) between repeated neighbor warning messages. The range is from 1 to 65535. The default is 10.

Command Default

Neighbor warning messages are logged at 10-second intervals.

Command Modes

Router configuration (config-router) Address-family configuration (config-router-af) Service-family configuration (config-router-sf)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

When neighbor warning messages occur, they are logged by default. With this command, you can disable and enable neighbor warning messages, and you can configure the interval between repeated neighbor warning messages.

To enable the logging of warning messages for an EIGRP address family, use the **eigrp log-neighbor-warnings** command in address-family configuration mode.

To enable the logging of warning messages for an EIGRP service family, use the **eigrp log-neighbor-warnings** command in service-family configuration mode.

Examples

The following command will log neighbor warning messages for EIGRP process 209 and repeat the warning messages in 5-minute (300 seconds) intervals:

```
Device(config)# router eigrp 209
Device(config-router)# eigrp log-neighbor-warnings 300
```

The following example logs neighbor warning messages for the service family with autonomous system number 4453 and repeats the warning messages in five-minute (300 second) intervals:

```
Device(config)# router eigrp virtual-name
Device(config-router)# service-family ipv4 autonomous-system 4453
Device(config-router-sf)# eigrp log-neighbor-warnings 300
```

The following example logs neighbor warning messages for the address family with autonomous system number 4453 and repeats the warning messages in five-minute (300 second) intervals:

```
Device(config)# router eigrp virtual-name
```

```
Device(config-router)# address-family ipv4 autonomous-system 4453
Device(config-router-af)# eigrp log-neighbor-warnings 300
```

Related Commands

Command	Description
address-family (EIGRP)	Enters address-family configuration mode to configure an EIGRP routing instance.
exit-address-family	Exits address-family configuration mode.
exit-service-family	Exits service-family configuration mode.
router eigrp	Configures the EIGRP routing process.
service-family	Specifies service-family configuration mode.

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

as-number	Autonomous system number to which the authentication applies.
key-chain	Name of the authentication key chain.

Command Default

No authentication is provided for EIGRP packets.

Command Modes

Interface configuration (config-if) Virtual network interface (config-if-vnet)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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

Command	Description
accept-lifetime	Sets the time period during which the authentication key on a key chain is received as valid.
ip authentication mode eigrp	Specifies the type of authentication used in EIGRP packets.
key	Identifies an authentication key on a key chain.
key chain	Enables authentication of routing protocols.
key-string (authentication)	Specifies the authentication string for a key.
send-lifetime	Sets the time period during which an authentication key on a key chain is valid to be sent.

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

as-number	Autonomous system number.
md5	Keyed Message Digest 5 (MD5) authentication.

Command Default

No authentication is provided for EIGRP packets.

Command Modes

Interface configuration (config-if) Virtual network interface (config-if-vnet)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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

Command	Description
accept-lifetime	Sets the time period during which the authentication key on a key chain is received as valid.
ip authentication key-chain eigrp	Enables authentication of EIGRP packets.
key	Identifies an authentication key on a key chain.
key chain	Enables authentication of routing protocols.
key-string (authentication)	Specifies the authentication string for a key.
send-lifetime	Sets the time period during which an authentication key on a key chain is valid to be sent.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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

Command	Description
bandwidth (interface)	Sets a bandwidth value for an interface.

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

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.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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

Command	Description
ip load-sharing	Enables load balancing for Cisco Express Forwarding.

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

list-name	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 **show ip prefix-list** command.
seq	(Optional) Applies a sequence number to a prefix-list entry.
number	(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.
deny	Denies access for a matching condition.
permit	Permits access for a matching condition.
network / length	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.
ge	(Optional) Specifies the lesser value of a range (the "from" portion of the range description) by applying the *ge-length* argument to the range specified. **Note** The **ge** keyword represents the greater than or equal to operator.
ge-length	(Optional) Represents the minimum prefix length to be matched.
le	(Optional) Specifies the greater value of a range (the "to" portion of the range description) by applying the *le-length* argument to the range specified. **Note** The **le** keyword represents the less than or equal to operator.
le-length	(Optional) Represents the maximum prefix length to be matched.
description	(Optional) Configures a descriptive name for the prefix list.
description	(Optional) Descriptive name of the prefix list, from 1 to 80 characters in length.
sequence-number	(Optional) Enables or disables the use of sequence numbers for prefix lists.

Command Default

No prefix lists or prefix-list entries are created.

Command Modes

Global configuration (config)

Command History

Table 113:

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

length <**ge** *ge-length* <**le** *le-length* <= 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

Command	Description
clear ip prefix-list	Resets the prefix list entry counters.
ip prefix-list description	Adds a text description of a prefix list.
ip prefix-list sequence	Enables or disables default prefix-list sequencing.
match ip address	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.
neighbor prefix-list	Filters routes from the specified neighbor using a prefix list.
show ip prefix-list	Displays information about a prefix list or prefix list entries.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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 109 10
```

Related Commands

Command	Description
bandwidth (interface)	Sets a bandwidth value for an interface.
ip hold-time eigrp	Configures the hold time for a particular EIGRP routing process designated by the autonomous system number.

ip hold-time eigrp

To configure the hold time for an Enhanced Interior Gateway Routing Protocol (EIGRP) process, use the **ip hold-time eigrp** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ip hold-time eigrp *as-number seconds*
no ip hold-time eigrp *as-number seconds*

Syntax Description

as-number	Autonomous system number.
seconds	Hold time (in seconds). The range is from 1 to 65535.

Command Default

The EIGRP hold time is 180 seconds for low-speed, nonbroadcast multiaccess (NBMA) networks and 15 seconds for all other networks.

Command Modes

Interface configuration (config-if) Virtual network interface (config-if-vnet)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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 **bandwidth** interface configuration command.

Examples

The following example sets the hold time for Ethernet interface 0 to 40 seconds:

```
Device(config)#interface ethernet 0
Device(config-if)#ip hold-time eigrp 109 40
```

Related Commands

Command	Description
bandwidth (interface)	Sets a bandwidth value for an interface.
ip hello-interval eigrp	Configures the hello interval for the EIGRP routing process designated by an autonomous system number.

ip load-sharing

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-destination** }
no ip load-sharing

Syntax Description

per-destination	Enables per-destination load balancing for Cisco Express Forwarding on the interface.

Command Default

Per-destination load balancing is enabled by default when you enable Cisco Express Forwarding.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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.

Examples

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 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

disable	(Optional) Disables the filtering of outgoing LSAs to an OSPF interface; all outgoing LSAs are flooded to the interface. **Note** This keyword is available only in virtual network interface mode.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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
```

Related Commands

Command	Description
neighbor database-filter	Filters outgoing LSAs to an OSPF neighbor.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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

Command	Description
ip split-horizon (RIP)	Enables the split horizon mechanism.
neighbor (EIGRP)	Defines a neighboring router with which to exchange routing information.

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

as-number	Autonomous system number.
ip-address	Summary IP address to apply to an interface.
mask	Subnet mask.
admin-distance	(Optional) Administrative distance. Range: 0 to 255. **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.
leak-map *name*	(Optional) Specifies the route-map reference that is used to configure the route leaking through the summary.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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

Command	Description
auto-summary (EIGRP)	Configures automatic summarization of subnet routes to network-level routes (default behavior).
summary-metric	Configures fixed metrics for an EIGRP summary aggregate address.

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

interface-type interface-number	Interface type and number.
ip-address	IP address of the gateway, in A.B.C.D format.
vrf *vrf-name*	Specifies Virtual Routing and Forwarding (VRF) instance and the destination vrf name.
group *group-name*	(Optional) Assigns a BFD group. The group-name is a character string of up to 32 characters specifying the BFD group name.
unassociate	(Optional) Unassociates the static route configured for a BFD.

Command Default

No static route BFD neighbors are specified.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Use the ip route static bfd command to specify static route BFD neighbors. All static routes that have the same interface and gateway specified in the configuration share the same BFD session for reachability notification.

All static routes that specify the same values for the interface-type, interface-number, and ip-address arguments will automatically use BFD to determine gateway reachability and take advantage of fast failure detection.

The **group** keyword assigns a BFD group. The static BFD configuration is added to the VPN routing and forwarding (VRF) instance with which the interface is associated. The **passive** keyword specifies the passive member of the group. Adding static BFD in a group without the passive keyword makes the BFD an active member of the group. A static route should be tracked by the active BFD configuration in order to trigger a BFD session for the group. To remove all the static BFD configurations (active and passive) of a specific group, use the **no ip route static bfd** command and specify the BFD group name.

The **unassociate** keyword specifies that a BFD neighbor is not associated with static route, and the BFD sessions are requested if an interface has been configured with BFD. This is useful in bringing up a BFDv4 session in the absence of an IPv4 static route. If the unassociate keyword is not provided, then the IPv4 static routes are associated with BFD sessions.

BFD requires that BFD sessions are initiated on both endpoint devices. Therefore, this command must be configured on each endpoint device.

The BFD static session on a switch virtual interface (SVI) is established only after the **bfd interval** *milliseconds* **min_rx** *milliseconds* **multiplier** *multiplier-value* command is disabled and enabled on that SVI.

To enable the static BFD sessions, perform the following steps:

1. Enable BFD timers on the SVI.

   bfd interval *milliseconds* **min_rx** *milliseconds* **multiplier** *multiplier-value*

2. Enable BFD for the static IP route

   ip route static bfd *interface-type interface-number ip-address*

3. Disable and enable the BFD timers on the SVI again.

   no bfd interval *milliseconds* **min_rx** *milliseconds* **multiplier** *multiplier-value*

   bfd interval *milliseconds* **min_rx** *milliseconds* **multiplier** *multiplier-value*

Examples

The following example shows how to configure BFD for all static routes through a specified neighbor, group, and active member of the group:

```
Device#configuration terminal
Device(config)#ip route static bfd GigabitEthernet 1/0/1 10.1.1.1 group group1
```

The following example shows how to configure BFD for all static routes through a specified neighbor, group, and passive member of the group:

```
Device#configuration terminal
Device(config)#ip route static bfd GigabitEthernet 1/0/1 10.2.2.2 group group1 passive
```

The following example shows how to configure BFD for all static routes in an unassociated mode without the group and passive keywords:

```
Device#configuration terminal
Device(config)#ip route static bfd GigabitEthernet 1/0/1 10.2.2.2 unassociate
```

ipv6 route static bfd

To specify static route Bidirectional Forwarding Detection for IPv6 (BFDv6) neighbors, use the **ipv6 route static bfd** command in global configuration mode. To remove a static route BFDv6 neighbor, use the**no** form of this command

ipv6 route static bfd [**vrf** *vrf-name*] *interface-type interface-number ipv6-address* **[unassociated]**
no ipv6 route static bfd

Syntax Description

vrf *vrf-name*	(Optional) Name of the virtual routing and forwarding (VRF) instance by which static routes should be specified.
interface-type interface-number	Interface type and number.
ipv6-address	IPv6 address of the neighbor.
unassociated	(Optional) Moves a static BFD neighbor from associated mode to unassociated mode.

Command Default

No static route BFDv6 neighbors are specified.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Use the ipv6 route static bfd command to specify static route neighbors. All of the static routes that have the same interface and gateway specified in the configuration share the same BFDv6 session for reachability notification. BFDv6 requires that BFDv6 sessions are initiated on both endpoint routers. Therefore, this command must be configured on each endpoint router. An IPv6 static BFDv6 neighbor must be fully specified (with the interface and the neighbor address) and must be directly attached.

All static routes that specify the same values for vrf vrf-name, interface-type interface-number , and *ipv6-address* will automatically use BFDv6 to determine gateway reachability and take advantage of fast failure detection.

Examples

The following example creates a neighbor on Ethernet interface 0/0 with an address of 2001::1:

```
Device#configuration terminal
Device(config)#ipv6 route static bfd ethernet 0/0 2001::1
```

The following example converts the neighbor to unassociated mode:

```
Device#configuration terminal
Device(config)#ipv6 route static bfd ethernet 0/0 2001::1 unassociated
```

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

Syntax Description

tos	Type of service. This value must always be zero.
k1 k2 k3 k4 k5 k6	(Optional) Constants that convert an EIGRP metric vector into a scalar quantity. Valid values are 0 to 255. Given below are the default values: • *k1:* 1 • *k2:* 0 • *k3:* 1 • *k4:* 0 • *k5:* 0 • *k6:* 0 **Note** In address family configuration mode, if the values are not specified, default values are configured. The *k6* argument is supported only in address family configuration mode.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

metric = [k1 * bandwidth + (k2 * bandwidth)/(256 – load) + k3 * delay + K6 * extended metrics]

If k5 does not equal zero, an additional operation is performed:

metric = metric * [k5/(reliability + k4)]

Scaled Bandwidth= 10^7/minimum interface bandwidth (in kilobits per second) * 256

Delay is in tens of microseconds for classic mode and pico seconds for named mode. In classic mode, a delay of hexadecimal FFFFFFFF (decimal 4294967295) indicates that the network is unreachable. In named mode, a delay of hexadecimal FFFFFFFFFFF (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

Command	Description
address-family (EIGRP)	Enters address family configuration mode to configure an EIGRP routing instance.
bandwidth (interface)	Sets a bandwidth value for an interface.
delay (interface)	Sets a delay value for an interface.
ipv6 router eigrp	Configures an IPv6 EIGRP routing process.
metric holddown	Keeps new EIGRP routing information from being used for a certain period of time.
metric maximum-hops	Causes IP routing software to advertise routes with a hop count higher than what is specified by the command (EIGRP only) as unreachable routes.
router eigrp	Configures an EIGRP routing process.

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-addresspeer-group-name*} **description** *text*
no neighbor {*ip-addresspeer-group-name*} **description** [*text*]

Syntax Description

ip-address	IP address of the neighbor.
peer-group-name	Name of an EIGRP peer group. This argument is not available in address-family configuration mode.
text	Text (up to 80 characters in length) that describes the neighbor.

Command Default

There is no description of the neighbor.

Command Modes

Router configuration (config-router) Address family configuration (config-router-af)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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

Command	Description
address-family (EIGRP)	Enters address family configuration mode to configure an EIGRP routing instance.
network (EIGRP)	Specifies the network for an EIGRP routing process.
router eigrp	Configures the EIGRP address family process.

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

ip-address	IP address of the directly connected network.
wildcard-mask	(Optional) EIGRP wildcard bits. Wildcard mask indicates a subnetwork, bitwise complement of the subnet mask.

Command Default

No networks are specified.

Command Modes

Router configuration (config-router) Address-family configuration (config-router-af)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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
```

Related Commands

Command	Description
address-family (EIGRP)	Enters address-family configuration mode to configure an EIGRP routing instance.
router eigrp	Configures the EIGRP address-family process.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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

Command	Description
debug eigrp address-family ipv6 notifications	Displays information about EIGRP address family IPv6 event notifications.
debug eigrp nsf	Displays notifications and information about NSF events for an EIGRP routing process.
debug ip eigrp notifications	Displays information and notifications for an EIGRP routing process.

Command	Description
show ip protocols	Displays the parameters and the current state of the active routing protocol process.
show ipv6 protocols	Displays the parameters and the current state of the active IPv6 routing protocol process.
timers graceful-restart purge-time	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.
timers nsf converge	Sets the maximum time that the restarting router must wait for the end-of-table notification from an NSF-capable or NSF-aware peer.
timers nsf signal	Sets the maximum time for the initial restart period.

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-numberaccess-list-name*} {**in** | **out**} *offset* [*interface-type interface-number*]
no offset-list {*access-list-numberaccess-list-name*} {**in** | **out**} *offset* [*interface-type interface-number*]

Syntax Description

access-list-number | *access-list-name*	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.
in	Applies the access list to incoming metrics.
out	Applies the access list to outgoing metrics.
offset	Positive offset to be applied to metrics for networks matching the access list. If the offset is 0, no action is taken.
interface-type	(Optional) Interface type to which the offset list is applied.
interface-number	(Optional) Interface number to which the offset list is applied.

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 114:

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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
```

redistribute (IP)

To redistribute routes from one routing domain into another routing domain, use the **redistribute** command in the appropriate configuration mode. To disable all or some part of the redistribution (depending on the protocol), use the **no** form of this command. See the "Usage Guidelines" section for detailed, protocol-specific behaviors.

redistribute *protocol* [*process-id*] {**level-1** | **level-1-2** | **level-2**} [*autonomous-system-number*] [**metric** {*metric-value* | **transparent**}] [**metric-type** *type-value*] [**match** {**internal** | **external 1** | **external 2**}] [**tag** *tag-value*] [**route-map** *map-tag*] [**subnets**] [**nssa-only**]
no redistribute *protocol* [*process-id*] {**level-1** | **level-1-2** | **level-2**} [*autonomous-system-number*] [**metric** {*metric-value* | **transparent**}] [**metric-type** *type-value*] [**match** {**internal** | **external 1** | **external 2**}] [**tag** *tag-value*] [**route-map** *map-tag*] [**subnets**] [**nssa-only**]

Syntax Description

protocol	Source protocol from which routes are being redistributed. It can be one of the following keywords: **application**, **bgp**, **connected**, **eigrp**, **isis**, **mobile**, **ospf**, **rip**, or **static** [**ip**]. The **static** [**ip**] keyword is used to redistribute IP static routes. The optional **ip** keyword is used when redistributing into the Intermediate System-to-Intermediate System (IS-IS) protocol. The **application** keyword is used to redistribute an application from one routing domain to another. You can redistribute more than one application to different routing protocols such as IS-IS, OSPF, Border Gateway Protocol (BGP), Enhanced Interior Gateway Routing Protocol (EIGRP) and Routing Information Protocol (RIP). The **connected** keyword refers to routes that are established automatically by virtue of having enabled IP on an interface. For routing protocols such as Open Shortest Path First (OSPF) and IS-IS, these routes will be redistributed as external to the autonomous system.

process-id	(Optional) For the **application** keyword, this is the name of an application. For the **bgp** or **eigrp** keyword, this is an autonomous system number, which is a 16-bit decimal number. For the **isis** keyword, this is an optional *tag* value that defines a meaningful name for a routing process. Creating a name for a routing process means that you use names when configuring routing. You can configure a router in two routing domains and redistribute routing information between these two domains. For the **ospf** keyword, this is an appropriate OSPF process ID from which routes are to be redistributed. This identifies the routing process. This value takes the form of a nonzero decimal number. For the **rip** keyword, no *process-id* value is needed. For the **application** keyword, this is the name of an application. By default, no process ID is defined.
level-1	Specifies that, for IS-IS, Level 1 routes are redistributed into other IP routing protocols independently.
level-1-2	Specifies that, for IS-IS, both Level 1 and Level 2 routes are redistributed into other IP routing protocols.
level-2	Specifies that, for IS-IS, Level 2 routes are redistributed into other IP routing protocols independently.
autonomous-system-number	(Optional) Autonomous system number for the redistributed route. The range is from 1 to 65535. • 4-byte autonomous system numbers are supported in the range from 1.0 to 65535.65535 in asdot notation only. For more details about autonomous system number formats, see the **router bgp** command.
metric *metric-value*	(Optional) When redistributing from one OSPF process to another OSPF process on the same router, the metric will be 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. The default value is 0.
metric transparent	(Optional) Causes RIP to use the routing table metric for redistributed routes as the RIP metric.

metric-type *type value*	(Optional) For OSPF, specifies the external link type associated with the default route advertised into the OSPF routing domain. It can be one of two values: • **1**—Type 1 external route • **2**—Type 2 external route If a **metric-type** is not specified, the Cisco IOS software adopts a Type 2 external route. For IS-IS, it can be one of two values: • **internal**—IS-IS metric that is < 63. • **external**—IS-IS metric that is > 64 < 128. The default is **internal**.
match {**internal** | **external1** | **external2**}	(Optional) Specifies the criteria by which OSPF routes are redistributed into other routing domains. It can be one of the following: • **internal**—Routes that are internal to a specific autonomous system. • **external 1**—Routes that are external to the autonomous system, but are imported into OSPF as Type 1 external routes. • **external 2**—Routes that are external to the autonomous system, but are imported into OSPF as Type 2 external routes. The default is **internal**.
tag *tag-value*	(Optional) Specifies the 32-bit decimal value attached to each external route. This is not used by OSPF itself. It may be used to communicate information between Autonomous System Boundary Routers (ASBRs). If none is specified, the remote autonomous system number is used for routes from BGP and Exterior Gateway Protocol (EGP); for other protocols, zero (0) is used.
route-map	(Optional) Specifies the route map that should be interrogated to filter the importation of routes from this source routing protocol to the current routing protocol. If not specified, all routes are redistributed. If this keyword is specified, but no route map tags are listed, no routes will be imported.
map-tag	(Optional) Identifier of a configured route map.

subnets	(Optional) For redistributing routes into OSPF. **Note** Irrespective of whether the **subnets** keyword is configured or not, the subnets functionality is enabled by default. This automatic addition results in the redistribution of classless OSPF routes.
nssa-only	(Optional) Sets the nssa-only attribute for all routes redistributed into OSPF.

Command Default

Route redistribution is disabled.

Command Modes

Router configuration (config-router)

Address family configuration (config-af)

Address family topology configuration (config-router-af-topology)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Using the no Form of the redistribute Command

Caution Removing options that you have configured for the **redistribute** command requires careful use of the **no** form of the **redistribute** command to ensure that you obtain the result that you are expecting. Changing or disabling any keyword may or may not affect the state of other keywords, depending on the protocol.

It is important to understand that different protocols implement the **no** form of the **redistribute** command differently:

- In BGP, OSPF, and RIP configurations, the **no redistribute** command removes only the specified keywords from the **redistribute** commands in the running configuration. They use the *subtractive keyword* method when redistributing from other protocols. For example, in the case of BGP, if you configure **no redistribute static route-map interior**, *only the route map* is removed from the redistribution, leaving **redistribute static** in place with no filter.
- The **no redistribute isis** command removes the IS-IS redistribution from the running configuration. IS-IS removes the entire command, regardless of whether IS-IS is the redistributed or redistributing protocol.
- EIGRP used the subtractive keyword method prior to EIGRP component version rel5. Starting with EIGRP component version rel5, the **no redistribute** command removes the entire **redistribute** command when redistributing from any other protocol.
- An EIGRP routing process is configured when you issue the **router eigrp** command and then specify a network for the process using the **network** sub-command. Suppose that you have not configured an EIGRP routing process, and that you have configured redistribution of routes from such an EIGRP process into BGP, OSPF, or RIP. If you use the **no redistribute eigrp** command to change or disable a parameter

in the **redistribute eigrp** command, the **no redistribute eigrp** command removes the entire **redistribute eigrp** command instead of changing or disabling a specific parameter.

Additional Usage Guidelines for the redistribute Command

A router receiving a link-state protocol with an internal metric will consider the cost of the route from itself to the redistributing router plus the advertised cost to reach the destination. An external metric only considers the advertised metric to reach the destination.

Routes learned from IP routing protocols can be redistributed 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.

Redistributed routing information must be filtered by the **distribute-list out** router configuration command. This guideline ensures that only those routes intended by the administrator are passed along to the receiving routing protocol.

Whenever you use the **redistribute** or the **default-information** router configuration commands to redistribute routes into an OSPF routing domain, the router automatically becomes an ASBR. However, an ASBR does not, by default, generate a default route into the OSPF routing domain.

When routes are redistributed into OSPF from protocols other than OSPF or BGP, and no metric has been specified with the **metric-type** keyword and *type-value* argument, OSPF will use 20 as the default metric. When routes are redistributed into OSPF from BGP, OSPF will use 1 as the default metric. When routes are redistributed from one OSPF process to another OSPF process, autonomous system external and not-so-stubby-area (NSSA) routes will use 20 as the default metric. When intra-area and inter-area routes are redistributed between OSPF processes, the internal OSPF metric from the redistribution source process is advertised as the external metric in the redistribution destination process. (This is the only case in which the routing table metric will be preserved when routes are redistributed into OSPF.)

Note The **show ip ospf** [**topology-info**] command will display **subnets** keyword irrespective of whether the **subnets** keyword is configured or not. This is because the subnets functionality is enabled by default for OSPF.

On a router internal to an NSSA area, the **nssa-only** keyword causes the originated type-7 NSSA LSAs to have their propagate (P) bit set to zero, which prevents area border routers from translating these LSAs into type-5 external LSAs. On an area border router that is connected to an NSSA and normal areas, the **nssa-only** keyword causes the routes to be redistributed only into the NSSA areas.

Routes configured with the **connected** keyword affected by this **redistribute** command are the routes not specified by the **network** router configuration command.

You cannot use the **default-metric** command to affect the metric used to advertise connected routes.

Note The **metric** value specified in the **redistribute** command supersedes the **metric** value specified in the **default-metric** command.

The default redistribution of Interior Gateway Protocol (IGP) or Exterior Gateway Protocol (EGP) into BGP is not allowed unless the **default-information originate** router configuration command is specified.

4-Byte Autonomous System Number Support

The Cisco implementation of 4-byte autonomous system numbers uses asplain—65538 for example—as the default regular expression match and output display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain format and the asdot format as described in RFC 5396. To change the default regular expression match and output display of 4-byte autonomous system numbers to asdot format, use the **bgp asnotation dot** command.

Examples

The following example shows how OSPF routes are redistributed into a BGP domain:

```
Device(config)# router bgp 109
Device(config-router)# redistribute ospf
```

The following example shows how to redistribute EIGRP routes into an OSPF domain:

```
Device(config)# router ospf 110
Device(config-router)# redistribute eigrp
```

The following example shows how to redistribute the specified EIGRP process routes into an OSPF domain. The EIGRP-derived metric will be remapped to 100 and RIP routes to 200.

```
Device(config)# router ospf 109
Device(config-router)# redistribute eigrp 108 metric 100 subnets
Device(config-router)# redistribute rip metric 200 subnets
```

The following example shows how to configure BGP routes to be redistributed into IS-IS. The link-state cost is specified as 5, and the metric type is set to external, indicating that it has lower priority than internal metrics.

```
Device(config)# router isis
Device(config-router)# redistribute bgp 120 metric 5 metric-type external
```

The following example shows how to redistribute an application into an OSPF domain and specify a metric value of 5:

```
Device(config)# router ospf 4
Device(config-router)# redistribute application am metric 5
```

In the following example, network 172.16.0.0 will appear as an external LSA in OSPF 1 with a cost of 100 (the cost is preserved):

```
Device(config)# interface ethernet 0
Device(config-if)# ip address 172.16.0.1 255.0.0.0
Device(config-if)# exit
Device(config)# ip ospf cost 100
Device(config)# interface ethernet 1
Device(config-if)# ip address 10.0.0.1 255.0.0.0
!
Device(config)# router ospf 1
Device(config-router)# network 10.0.0.0 0.255.255.255 area 0
Device(config-if)# exit
Device(config-router)# redistribute ospf 2 subnet
Device(config)# router ospf 2
Device(config-router)# network 172.16.0.0 0.255.255.255 area 0
```

The following example shows how BGP routes are redistributed into OSPF and assigned the local 4-byte autonomous system number in asplain format.

```
Device(config)# router ospf 2
Device(config-router)# redistribute bgp 65538
```

The following example shows how to remove the **connected metric 1000 subnets** options from the **redistribute connected metric 1000 subnets** command and leave the **redistribute connected** command in the configuration:

```
Device(config-router)# no redistribute connected metric 1000 subnets
```

The following example shows how to remove the **metric 1000** options from the **redistribute connected metric 1000 subnets** command and leave the **redistribute connected subnets** command in the configuration:

```
Device(config-router)# no redistribute connected metric 1000
```

The following example shows how to remove the **subnets** option from the **redistribute connected metric 1000 subnets** command and leave the **redistribute connected metric 1000** command in the configuration:

```
Device(config-router)# no redistribute connected subnets
```

The following example shows how to remove the **redistribute connected** command, and any of the options that were configured for the **redistribute connected** command, from the configuration:

```
Device(config-router)# no redistribute connected
```

The following example shows how EIGRP routes are redistributed into an EIGRP process in a named EIGRP 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)# redistribute eigrp 6473 metric 1 1 1 1 1
```

The following example shows how to set and disable the redistributions in EIGRP configuration. Note that, in the case of EIGRP, the **no** form of the commands removes the entire set of **redistribute** commands from the running configuration.

```
Device(config)# router eigrp 1
Device(config-router)# network 0.0.0.0
Device(config-router)# redistribute eigrp 2 route-map x
Device(config-router)# redistribute ospf 1 route-map x
Device(config-router)# redistribute bgp 1 route-map x
Device(config-router)# redistribute isis level-2 route-map x
Device(config-router)# redistribute rip route-map x

Device(config)# router eigrp 1
Device(config-router)# no redistribute eigrp 2 route-map x
Device(config-router)# no redistribute ospf 1 route-map x
Device(config-router)# no redistribute bgp 1 route-map x
Device(config-router)# no redistribute isis level-2 route-map x
Device(config-router)# no redistribute rip route-map x
Device(config-router)# end

Device# show running-config | section router eigrp 1

router eigrp 1
```

```
 network 0.0.0.0
```

The following example shows how to set and disable the redistributions in OSPF configuration. Note that the **no** form of the commands removes only the specified keywords from the **redistribute** command in the running configuration.

```
Device(config)# router ospf 1
Device(config-router)# network 0.0.0.0
Device(config-router)# redistribute eigrp 2 route-map x
Device(config-router)# redistribute ospf 1 route-map x
Device(config-router)# redistribute bgp 1 route-map x
Device(config-router)# redistribute isis level-2 route-map x
Device(config-router)# redistribute rip route-map x

Device(config)# router ospf 1
Device(config-router)# no redistribute eigrp 2 route-map x
Device(config-router)# no redistribute ospf 1 route-map x
Device(config-router)# no redistribute bgp 1 route-map x
Device(config-router)# no redistribute isis level-2 route-map x
Device(config-router)# no redistribute rip route-map x
Device(config-router)# end

Device# show running-config | section router ospf 1

router ospf 1
 redistribute eigrp 2
 redistribute ospf 1
 redistribute bgp 1
 redistribute rip
 network 0.0.0.0
```

The following example shows how to remove only the route map filter from the redistribution in BGP; redistribution itself remains in force without a filter:

```
Device(config)# router bgp 65000
Device(config-router)# no redistribute eigrp 2 route-map x
```

The following example shows how to remove the EIGRP redistribution to BGP:

```
Device(config)# router bgp 65000
Device(config-router)# no redistribute eigrp 2
```

Related Commands

Command	Description
default-information originate (OSPF)	Generates a default route into an OSPF routing domain.
router bgp	Configures the BGP routing process.
router eigrp	Configures the EIGRP address-family process.

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

protocol	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**.
process-id	(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.
include-connected	(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.
level-1	Specifies that for IS-IS, Level 1 routes are redistributed into other IPv6 routing protocols independently.
level-1-2	Specifies that for IS-IS, both Level 1 and Level 2 routes are redistributed into other IPv6 routing protocols.
level-2	Specifies that for IS-IS, Level 2 routes are redistributed into other IPv6 routing protocols independently.
as-number	(Optional) Autonomous system number for the redistributed route.
metric *metric-value*	(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.

metric-type *type-value*	(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: • **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 *tag-value*	(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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command w

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.

Note 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

Release	Modificati
Cisco IOS XE Fuji 16.9.2	This comm

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).

Examples

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
```

route-map

To define conditions for redistributing routes from one routing protocol to another routing protocol, or to enable policy routing, use the **route-map** command in global configuration mode. To delete an entry, use the **no** form of this command.

route-map *map-tag* [{**permit** | **deny**}] [*sequence-number*] **ordering-seq** *sequence-name*
no route-map *map-tag* [{**permit** | **deny**}] [*sequence-number*] **ordering-seq** *sequence-name*

Syntax Description

map-tag	Name for the route map.
permit	(Optional) Permits only the routes matching the route map to be forwarded or redistributed.
deny	(Optional) Blocks routes matching the route map from being forwarded or redistributed.
sequence-number	(Optional) Number that indicates the position a new route map will have in the list of route maps already configured with the same name.
ordering-seq *sequence-name*	(Optional) Orders the route maps based on the string provided.

Command Default

Policy routing is not enabled, and conditions for redistributing routes from one routing protocol to another routing protocol are not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Use the **route-map** command to enter route-map configuration mode.

Use route maps to redistribute routes, or to subject packets to policy routing. Both these purposes are described here.

Redistribution

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 to another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*, that is, the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the *set actions*, that is, the redistribution actions to be performed if the criteria enforced by the **match** commands are met. If the **route-map** command is enabled and the user does not specify any action, then the **permit** action is applied by default. The **no route-map** command deletes the route map.

The **match** route-map configuration command has multiple formats. The **match** commands can be run in any order, and all the **match** commands must match to cause the route to be redistributed according to the *set actions* specified with the **set** commands. The **no** forms of the **match** commands remove the specified match criteria.

Use route maps when you want detailed control over how routes are redistributed between routing processes. The destination routing protocol is the one you specify with the **router** global configuration command. The source routing protocol is the one you specify with the **redistribute** router configuration command. See the examples section for an illustration of how route maps are configured.

When passing routes through a route map, the route map can have several parts. Any route that does not match at least one **match** clause relating to a **route-map** command is ignored, that is, the route is not advertised for outbound route maps, and is not accepted for inbound route maps. If you want to modify only some data, configure a second route map section with an explicit match specified.

The **redistribute** router configuration command uses the name specified by the *map-tag* argument to reference a route map. Multiple route maps can share the same map tag name.

If the match criteria are met for this route map, and the **permit** keyword is specified, the route is redistributed as controlled by the set actions. In the case of policy routing, the packet is policy routed. If the match criteria are not met, and the **permit** keyword is specified, the next route map with the same map tag is tested. If a route passes none of the match criteria for the set of route maps sharing the same name, it is not redistributed by that set.

If the match criteria are met for the route map, and the **deny** keyword is specified, the route is not redistributed. In the case of policy routing, the packet is not policy routed, and no other route maps sharing the same map tag name are examined. If the packet is not policy routed, the normal forwarding algorithm is used.

Policy Routing

Another purpose of route maps is to enable policy routing. Use the **ip policy route-map** or **ipv6 policy route-map** command in addition to the **route-map** command, and the **match** and **set** commands to define the conditions for policy-routing packets. The **match** commands specify the conditions under which policy routing occurs. The **set** commands specify the routing actions to be performed if the criteria enforced by the **match** commands are met. We recommend that you policy route packets some way other than the obvious shortest path.

The *sequence-number* argument works as follows:

- If no entry is defined with the supplied tag, an entry is created with the *sequence-number* argument set to 10.
- If only one entry is defined with the supplied tag, that entry becomes the default entry for the **route-map** command. The *sequence-number* argument of this entry is unchanged.
- If more than one entry is defined with the supplied tag, an error message is displayed to indicate that the *sequence-number* argument is required.

If the **no route-map** *map-tag* command is specified (without the *sequence-number* argument), the entire route map is deleted.

Examples

The following example shows how to redistribute Routing Information Protocol (RIP) routes with a hop count equal to 1 to the Open Shortest Path First (OSPF). These routes will be redistributed to the OSPF as external link-state advertisements (LSAs) with a metric of 5, metric type of type1, and a tag equal to 1.

```
Device> enable
Device# configure terminal
Device(config)# router ospf 109
Device(config-router)# redistribute rip route-map rip-to-ospf
Device(config-router)# exit
Device(config)# route-map rip-to-ospf permit
```

```
Device(config-route-map)# match metric 1
Device(config-route-map)# set metric 5
Device(config-route-map)# set metric-type type1
Device(config-route-map)# set tag 1
```

The following example for IPv6 shows how to redistribute RIP routes with a hop count equal to 1 to the OSPF. These routes will be redistributed to the OSPF as external LSAs, with a tag equal to 42, and a metric type equal to type1.

```
Device> enable
Device# configure terminal
Device(config)# ipv6 router ospf 1
Device(config-router)# redistribute rip one route-map rip-to-ospfv3
Device(config-router)# exit
Device(config)# route-map rip-to-ospfv3
Device(config-route-map)# match tag 42
Device(config-route-map)# set metric-type type1
```

The following named configuration example shows how to redistribute Enhanced Interior Gateway Routing Protocol (EIGRP) addresses with a hop count equal to 1. These addresses are redistributed to the EIGRP as external, with a metric of 5, and a tag equal to 1:

```
Device> enable
Device# configure terminal
Device(config)# router eigrp virtual-name1
Device(config-router)# address-family ipv4 autonomous-system 4453
Device(config-router-af)# topology base
Device(config-router-af-topology)# redistribute eigrp 6473 route-map
virtual-name1-to-virtual-name2
Device(config-router-af-topology)# exit-address-topology
Device(config-router-af)# exit-address-family
Device(config-router)# router eigrp virtual-name2
Device(config-router)# address-family ipv4 autonomous-system 6473
Device(config-router-af)# topology base
Device(config-router-af-topology)# exit-af-topology
Device(config-router-af)# exit-address-family
Device(config)# route-map virtual-name1-to-virtual-name2
Device(config-route-map)# match tag 42
Device(config-route-map)# set metric 5
Device(config-route-map)# set tag 1
```

Related Commands

Command	Description
ip policy route-map	Identifies a route map to use for policy routing on an interface.
ipv6 policy route-map	Configures IPv6 PBR on an interface.
match	Matches values from the routing table.
router eigrp	Configures the EIGRP address-family process.
set	Sets values in the destination routing protocol
show route-map	Displays all route maps configured or only the one specified.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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

Command	Description
clear ip ospf	Clears redistribution based on the OSPF routing process ID.
router ospf	Configures the OSPF routing process.

router eigrp

To configure the 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-numbervirtual-instance-name*}
no router eigrp {*autonomous-system-numbervirtual-instance-name*}

Syntax Description

autonomous-system-number	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.
virtual-instance-name	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.

Command Default

No EIGRP processes are configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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
```

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*}]

Syntax Description

process-id	(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.

Command Default

OSPFv3 routing process is disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduce

Usage Guidelines

Use the **router ospfv3** command to enter OSPFv3 router configuration mode. From this mode, you can enter taddress-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

Command	Description
address-family ipv6	Enters IPv6 address family configuration mode.

send-lifetime

To set the time period during which an authentication key on a key chain is valid to be sent, use the **send-lifetime** command in key chain key configuration mode. To revert to the default value, use the **no** form of this command.

send-lifetime [**local**] *start-time* { **infinite** *end-time* | **duration** *seconds* }
no send-lifetime

Syntax Description

local	Specifies the time in local timezone.
start-time	Beginning time that the key specified by the **key** command is valid to be sent. The syntax can be either of the following: *hh* **:** *mm* **:** *ss month date year* *hh* **:** *mm* **:** *ss date month year* • *hh*: Hours • *mm*: Minutes • *ss*: Seconds • *month*: First three letters of the month • *date*: Date (1-31) • *year*: Year (four digits) The default start time and the earliest acceptable date is January 1, 1993.
infinite	Key is valid to be sent from the *start-time* value on.
end-time	Key is valid to be sent from the *start-time* value until the *end-time*value. The syntax is the same as that for the *start-time*value**.**The *end-time* value must be after the *start-time*value. The default end time is an infinite time period.
duration *seconds*	Length of time (in seconds) that the key is valid to be sent. The range is from 1 to 864000.

Command Default

Forever (the starting time is January 1, 1993, and the ending time is infinite)

Command Modes

Key chain key configuration (config-keychain-key)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Specify a *start-time* value and one of the following values: **infinite**, *end-time*, or **duration** *seconds*.

We recommend running Network Time Protocol (NTP) or some other time synchronization method if you intend to set lifetimes on keys.

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.

Examples

The following example configures a key chain named chain1. The key named key1 will be accepted from 1:30 p.m. to 3:30 p.m. and be sent from 2:00 p.m. to 3:00 p.m. The key named key2 will be accepted from 2:30 p.m. to 4:30 p.m. and be sent from 3:00 p.m. to 4:00 p.m. The overlap allows for migration of keys or a discrepancy in the set time of the router. There is a 30-minute leeway on each side to handle time differences.

```
Device(config)# interface GigabitEthernet1/0/1
Device(config-if)# ip rip authentication key-chain chain1
Device(config-if)# ip rip authentication mode md5
Device(config-if)# exit
Device(config)# router rip
Device(config-router)# network 172.19.0.0
Device(config-router)# version 2
Device(config-router)# exit
Device(config)# key chain chain1
Device(config-keychain)# key 1
Device(config-keychain-key)# key-string key1
Device(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 1996 duration 7200
Device(config-keychain-key)# send-lifetime 14:00:00 Jan 25 1996 duration 3600
Device(config-keychain-key)# exit
Device(config-keychain)# key 2
Device(config-keychain)# key-string key2
Device(config-keychain)# accept-lifetime 14:30:00 Jan 25 1996 duration 7200
Device(config-keychain)# send-lifetime 15:00:00 Jan 25 1996 duration 3600
```

The following example configures a key chain named chain1 for EIGRP address-family. The key named key1 will be accepted from 1:30 p.m. to 3:30 p.m. and be sent from 2:00 p.m. to 3:00 p.m. The key named key2 will be accepted from 2:30 p.m. to 4:30 p.m. and be sent from 3:00 p.m. to 4:00 p.m. The overlap allows for migration of keys or a discrepancy in the set time of the router. There is a 30-minute leeway on each side to handle time differences.

```
Device(config)# router eigrp 10
Device(config-router)# address-family ipv4 autonomous-system 4453
Device(config-router-af)# network 10.0.0.0
Device(config-router-af)# af-interface ethernet0/0
Device(config-router-af-interface)# authentication key-chain trees
Device(config-router-af-interface)# authentication mode md5
Device(config-router-af-interface)# exit
Device(config-router-af)# exit
Device(config-router)# exit
Device(config)# key chain chain1
Device(config-keychain)# key 1
Device(config-keychain-key)# key-string key1
Device(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 1996 duration 7200
Device(config-keychain-key)# send-lifetime 14:00:00 Jan 25 1996 duration 3600
Device(config-keychain-key)# exit
Device(config-keychain)# key 2
Device(config-keychain-key)# key-string key2
Device(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 1996 duration 7200
Device(config-keychain-key)# send-lifetime 15:00:00 Jan 25 1996 duration 3600
```

Related Commands

Command	Description
accept-lifetime	Sets the time period during which the authentication key on a key chain is received as valid.

Command	Description
key	Identifies an authentication key on a key chain.
key chain	Defines an authentication key chain needed to enable authentication for routing protocols.
key-string (authentication)	Specifies the authentication string for a key.
show key chain	Displays authentication key information.

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**}]

Syntax Description

vrf *vrf-name*	(Optional) Displays information about the specified virtual routing and forwarding (VRF) instance.
autonomous-system-number	(Optional) Autonomous system number whose output needs to be filtered.
type	(Optional) Interface type. For more information, use the question mark (?) online help function.
number	(Optional) Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
detail	(Optional) Displays detailed information about EIGRP interfaces for a specific EIGRP process.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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
```

```
Interface   Peers   Un/Reliable   SRTT   Un/Reliable   Flow Timer  Routes
Di0           0         0/0          0      11/434          0          0
Et0           1         0/0        337       0/10           0          0
SE0:1.16      1         0/0         10       1/63         103          0
Tu0           1         0/0        330       0/16           0          0
```

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)
                        Xmit Queue   PeerQ        Mean   Pacing Time   Multicast   Pending

Interface        Peers  Un/Reliable  Un/Reliable  SRTT   Un/Reliable   Flow Timer   Routes
Et0/0              1        0/0       0/0         525       0/2         3264           0
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)
                        Xmit Queue   PeerQ        Mean   Pacing Time   Multicast   Pending

Interface        Peers  Un/Reliable  Un/Reliable  SRTT   Un/Reliable   Flow Timer   Routes
Tu0/0              2        0/0       0/0           2       0/0          50           0
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 115: show ip eigrp interfaces Field Descriptions

Field	Description
Interface	Interface on which EIGRP is configured.
Peers	Number of directly connected EIGRP neighbors.

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

Command	Description
show eigrp address-family interfaces	Displays information about address family interfaces configured for EIGRP.
show ip eigrp neighbors	Displays neighbors discovered by EIGRP.

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

vrf *vrf-name*	(Optional) Displays information about the specified VPN Routing and Forwarding (VRF) instance.
autonomous-system-number	(Optional) Autonomous-system-number-specific output is displayed.
static	(Optional) Displays static neighbors.
detail	(Optional) Displays detailed neighbor information.
interface-type interface-number	(Optional) Interface-specific output is displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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
                                            (sec)         (ms)       Cnt Num
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 116: show ip eigrp neighbors Field Descriptions

Field	Description
Address	IP address of the EIGRP peer.
Interface	Interface on which the router is receiving hello packets from the peer.

Field	Description
Hold	Time in seconds for which EIGRP waits to hear from the peer before declaring it down.
Uptime	Elapsed time (in hours:minutes: seconds) since the local router first heard from this neighbor.
SRTT	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.
RTO	Retransmission timeout (in milliseconds). This is the amount of time the software waits before resending a packet from the retransmission queue to a neighbor.
Q Cnt	Number of EIGRP packets (update, query, and reply) that the software is waiting to send.
Seq Num	Sequence number of the last update, query, or reply packet that was received from this neighbor.

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 117: show ip eigrp neighbors detail Field Descriptions

Field	Description
H	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.
Address	IP address of the EIGRP peer.
Interface	Interface on which the router is receiving hello packets from the peer.
Hold	Time in seconds for which EIGRP waits to hear from the peer before declaring it down.
Lisp Encap	Indicates that routes from this neighbor are LISP encapsulated.
Uptime	Elapsed time (in hours:minutes: seconds) since the local router first heard from this neighbor.
SRTT	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.
RTO	Retransmission timeout (in milliseconds). This is the amount of time the software waits before resending a packet from the retransmission queue to a neighbor.
Q Cnt	Number of EIGRP packets (update, query, and reply) that the software is waiting to send.

Field	Description
Seq Num	Sequence number of the last update, query, or reply packet that was received from this neighbor.
Version	The software version that the specified peer is running.
Retrans	Number of times that a packet has been retransmitted.
Retries	Number of times an attempt was made to retransmit a packet.

Related Commands

Command	Description
show eigrp address-family neighbors	Displays neighbors discovered by EIGRP.

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 [{ *network* [{ *mask* }] *prefix* | **active** | **all-links** | **detail-links** | **pending** | **secondary-paths** | **summary** | **zero-successors** }]

Syntax Description

network	(Optional) Network address.
mask	(Optional) Network mask.
prefix	(Optional) Network prefix in the format <*network*>/<*length*>, for example, 192.168.0.0/16.
active	(Optional) Displays all topology entries that are in the active state.
all-links	(Optional) Displays all the entries in the EIGRP topology table (including nonfeasible successor sources).
detail-links	(Optional) Displays all the topology entries with additional details.
pending	(Optional) Displays all the entries in the EIGRP topology table that are either waiting for an update from a neighbor or to reply to a neighbor.
secondary-paths	(Optional) Displays the secondary paths in the topology.
summary	(Optional) Displays a summary of the EIGRP topology table.
zero-successors	(Optional) Displays the available routes that have zero successors.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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 the 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 that you use the **show eigrp address-family topology** command.

Examples

The following is a 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 192.16.1.0/24, 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 is a sample output from the **show ip eigrp topology** *prefix* command, and 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 is a sample output from the **show ip eigrp topology** *prefix* command, and displays detailed information about a single prefix. The prefix shown is an EIGRP external route.

```
Device# show ip eigrp topology 192.16.1.0/24

EIGRP-IPv4 Topology Entry for AS(1)/ID(10.0.0.1) for 192.16.1.0/24
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 192.16.1.0/24
        External data:
        AS number of route is 0
        External protocol is Connected, external metric is 0
        Administrator tag is 0 (0x00000000)
```

The following is a 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 is advertised as the default path over all the interfaces, and `ECMP Mode: Advertise by default` is displayed in the output. If any path other than the default path is advertised, `ECMP Mode: Advertise out <Interface name>` is 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 the 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 ½55
        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 ½55
        Minimum MTU is 1400
        Hop count is 1
        Originating router is 10.10.2.2
        ECMP Mode: Advertise out Tunnel1
```

The following is a sample output from the **show ip eigrp topology all-links** command, and displays all the paths, including 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 is a sample output from the **show ip eigrp topology detail-links** command, and 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 following table describes the significant fields shown in the above examples:

Table 118: show ip eigrp topology Field Descriptions

Field	Description
Codes	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. • P - Passive: Indicates that no EIGRP computations are being performed for this route. • A - Active: Indicates that EIGRP computations are being performed for this route. • U - Update: Indicates that a pending update packet is waiting to be sent for this route. • Q - Query: Indicates that a pending query packet is waiting to be sent for this route. • R - Reply: Indicates that a pending reply packet is waiting to be sent for this route. • r - Reply status: Indicates that EIGRP has sent a query for the route and is waiting for a reply from the specified path. • s - sia status: Indicates that the EIGRP query packet is in stuck-in-active (SIA) status.
successors	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.
serno	Serial number.
FD	Feasible distance. This 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.
via	Next-hop address that advertises the passive route.

Related Commands

Command	Description
show eigrp address-family topology	Displays entries in the EIGRP address-family topology 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

vrf *vrf-name*	(Optional) Displays information about the specified VRF.
vrf *	(Optional) Displays information about all VRFs.
autonomous-system-number	(Optional) Autonomous system number.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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 119: show ip eigrp traffic Field Descriptions

Field	Description
Hellos sent/received	Number of hello packets sent and received.
Updates sent/received	Number of update packets sent and received.
Queries sent/received	Number of query packets sent and received.

Field	Description
Replies sent/received	Number of reply packets sent and received.
Acks sent/received	Number of acknowledgement packets sent and received.
SIA-Queries sent/received	Number of stuck in active query packets sent and received.
SIA-Replies sent/received	Number of stuck in active reply packets sent and received.
Hello Process ID	Hello process identifier.
PDM Process ID	Protocol-dependent module IOS process identifier.
Socket Queue	The IP to EIGRP Hello Process socket queue counters.
Input queue	The EIGRP Hello Process to EIGRP PDM socket queue counters.

Related Commands

Command	Description
show eigrp address-family traffic	Displays the number of EIGRP packets sent and received.

show ip ospf

To display general information about Open Shortest Path First (OSPF) routing processes, use the **showipospf** command in user EXEC or privileged EXEC mode.

show ip ospf [*process-id*]

Syntax Description

process-id	(Optional) Process ID. If this argument is included, only information for the specified routing process is included.

Command Modes

User EXEC Privileged EXEC

Command History

Mainline Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Examples

The following is sample output from the **showipospf** 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 SPFs 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
```

```
        Number of indication LSA 1
        Number of DoNotAge LSA 0
        Flood list length 0
```

Cisco IOS Release 12.2(18)SXE, 12.0(31)S, and 12.4(4)T

The following is sample output from the **showipospf**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 SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 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 areas 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 120: show ip ospf Field Descriptions

Field	Description
Routing process “ospf 201” with ID 10.0.0.1	Process ID and OSPF router ID.
Supports...	Number of types of service supported (Type 0 only).
SPF schedule delay	Delay time (in seconds) of SPF calculations.
Minimum LSA interval	Minimum interval (in seconds) between link-state advertisements.

Field	Description
LSA group pacing timer	Configured LSA group pacing timer (in seconds).
Interface flood pacing timer	Configured LSA flood pacing timer (in milliseconds).
Retransmission pacing timer	Configured LSA retransmission pacing timer (in milliseconds).
Number of external LSA	Number of external link-state advertisements.
Number of opaque AS LSA	Number of opaque link-state advertisements.
Number of DCbitless external and opaque AS LSA	Number of demand circuit external and opaque link-state advertisements.
Number of DoNotAge external and opaque AS LSA	Number of do not age external and opaque link-state advertisements.
Number of areas in this router is	Number of areas configured for the router.
External flood list length	External flood list length.
BFD is enabled	BFD has been enabled on the OSPF process.

The following is an excerpt of output from the **showipospf** 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 SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 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 121: show ip ospf Field Descriptions

Field	Description
Area	OSPF area and tag.
Number of interfaces...	Number of interfaces configured in the area.
It is...	Possible types are internal, area border, or autonomous system boundary.
Routing process “ospf 1” with ID 192.168.0.1	Process ID and OSPF router ID.
Supports...	Number of types of service supported (Type 0 only).
Initial SPF schedule delay	Delay time of SPF calculations at startup.
Minimum hold time	Minimum hold time (in milliseconds) between consecutive SPF calculations.
Maximum wait time	Maximum wait time (in milliseconds) between consecutive SPF calculations.
Incremental-SPF	Status of incremental SPF calculations.
Minimum LSA...	Minimum time interval (in seconds) between link-state advertisements, and minimum arrival time (in milliseconds) of link-state advertisements,
LSA group pacing timer	Configured LSA group pacing timer (in seconds).
Interface flood pacing timer	Configured LSA flood pacing timer (in milliseconds).
Retransmission pacing timer	Configured LSA retransmission pacing timer (in milliseconds).
Number of...	Number and type of link-state advertisements that have been received.
Number of external LSA	Number of external link-state advertisements.
Number of opaque AS LSA	Number of opaque link-state advertisements.
Number of DCbitless external and opaque AS LSA	Number of demand circuit external and opaque link-state advertisements.
Number of DoNotAge external and opaque AS LSA	Number of do not age external and opaque link-state advertisements.
Number of areas in this router is	Number of areas configured for the router listed by type.
External flood list length	External flood list length.

The following is sample output from the **showipospf** command. In this example, the user had configured the **redistributionmaximum-prefix** command to set a limit of 2000 redistributed routes. SPF throttling was configured with the **timersthrottlespf** 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 122: show ip ospf Field Descriptions

Field	Description
Routing process “ospf 1” with ID 10.0.0.1	Process ID and OSPF router ID.
Supports ...	Number of Types of Service supported.
It is ...	Possible types are internal, area border, or autonomous system boundary router.
Redistributing External Routes from	Lists of redistributed routes, by protocol.
Maximum limit of redistributed prefixes	Value set in the **redistributionmaximum-prefix** command to set a limit on the number of redistributed routes.
Threshold for warning message	Percentage set in the **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.
Initial SPF schedule delay	Delay (in milliseconds) before initial SPF schedule for SPF throttling. Configured with the **timersthrottlespf** command.
Minimum hold time between two consecutive SPFs	Minimum hold time (in milliseconds) between two consecutive SPF calculations for SPF throttling. Configured with the **timersthrottlespf** command.
Maximum wait time between two consecutive SPFs	Maximum wait time (in milliseconds) between two consecutive SPF calculations for SPF throttling. Configured with the **timersthrottlespf** command.
Number of areas	Number of areas in router, area addresses, and so on.

The following is sample output from the **showipospf** 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
```

The following is sample **showipospf**command. In this example, the user had configured the **redistributionmaximum-prefix** command to set a limit of 2000 redistributed routes. SPF throttling was configured with the **timersthrottlespf** 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 123: show ip ospf Field Descriptions

Field	Description
Routing process “ospf 1” with ID 192.168.0.0.	Process ID and OSPF router ID.
Supports ...	Number of TOS supported.
It is ...	Possible types are internal, area border, or autonomous system boundary routers.
Redistributing External Routes from	Lists of redistributed routes, by protocol.
Maximum limit of redistributed prefixes	Value set in the **redistributionmaximum-prefix** command to set a limit on the number of redistributed routes.
Threshold for warning message	Percentage set in the **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.
Initial SPF schedule delay	Delay (in milliseconds) before the initial SPF schedule for SPF throttling. Configured with the **timersthrottlespf** command.
Minimum hold time between two consecutive SPFs	Minimum hold time (in milliseconds) between two consecutive SPF calculations for SPF throttling. Configured with the **timersthrottlespf** command.
Maximum wait time between two consecutive SPFs	Maximum wait time (in milliseconds) between two consecutive SPF calculations for SPF throttling. Configured with the **timersthrottlespf** command.
Number of areas	Number of areas in router, area addresses, and so on.

The following is sample output from the **showipospf** 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 **showipospfborder-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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Examples

The following is sample output from the **showipospfborder-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 124: **show ip ospf border-routers** Field Descriptions*

Field	Description
192.168.97.53	Router ID of the destination.
[10]	Cost of using this route.
via 172.16.1.53	Next hop toward the destination.
Serial0	Interface type for the outgoing interface.
ABR	The router type of the destination; it is either an ABR or ASBR or both.
Area	The area ID of the area from which this route is learned.
SPF 3	The internal number of the shortest path first (SPF) calculation that installs this route.

show ip ospf database

To display lists of information related to the Open Shortest Path First (OSPF) database for a specific router, use the **showipospfdatabase** command in EXEC mode.

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

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.
area-id	(Optional) Area number associated with the OSPF address range defined in the **network** router configuration command used to define the particular area.
adv-router [*ip-address*	(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**).

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The various forms of this command deliver information about different OSPF link state advertisements.

Examples

The following is sample output from the **showipospfdatabase** 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
```

```
172.16.21.5   172.16.21.5    1112    0x800009D2    0xA2B8       5
172.16.1.2    172.16.1.2     1662    0x80000A98    0x4CB6       9
172.16.1.1    172.16.1.1     1115    0x800009B6    0x5F2C       1
172.16.1.5    172.16.1.5     1691    0x80002BC     0x2A1A       5
172.16.65.6   172.16.65.6    1395    0x80001947    0xEEE1       4
172.16.241.5  172.16.241.5   1161    0x8000007C    0x7C70       1
172.16.27.6   172.16.27.6    1723    0x80000548    0x8641       4
172.16.70.6   172.16.70.6    1485    0x80000B97    0xEB84       6
               Displaying Net Link States(Area 0.0.0.0)
  Link ID       ADV Router      Age         Seq#       Checksum
172.16.1.3  192.168.239.66     1245    0x800000EC      0x82E
               Displaying Summary Net Link States(Area 0.0.0.0)
  Link ID       ADV Router       Age         Seq#       Checksum
172.16.240.0   172.16.241.5    1152      0x80000077      0x7A05
172.16.241.0   172.16.241.5    1152      0x80000070      0xAEB7
172.16.244.0   172.16.241.5    1152      0x80000071      0x95CB
```

The table below describes the significant fields shown in the display.

Table 125: show ip ospf Database Field Descriptions

Field	Description
Link ID	Router ID number.
ADV Router	Advertising router's ID.
Age	Link state age.
Seq#	Link state sequence number (detects old or duplicate link state advertisements).
Checksum	Fletcher checksum of the complete contents of the link state advertisement.
Link count	Number of interfaces detected for router.

The following is sample output from the **showipospfdatabase**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 126: show ip ospf database asbr-summary Field Descriptions

Field	Description
OSPF Router with id	Router ID number.
Process ID	OSPF process ID.

Field	Description
LS age	Link state age.
Options	Type of service options (Type 0 only).
LS Type	Link state type.
Link State ID	Link state ID (autonomous system boundary router).
Advertising Router	Advertising router's ID.
LS Seq Number	Link state sequence (detects old or duplicate link state advertisements).
Checksum	LS checksum (Fletcher checksum of the complete contents of the link state advertisement).
Length	Length in bytes of the link state advertisement.
Network Mask	Network mask implemented.
TOS	Type of service.
Metric	Link state metric.

The following is sample output from the **showipospfdatabase**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 127: show ip ospf database external Field Descriptions

Field	Description
OSPF Router with id	Router ID number.
Autonomous system	OSPF autonomous system number (OSPF process ID).
LS age	Link state age.
Options	Type of service options (Type 0 only).

Field	Description
LS Type	Link state type.
Link State ID	Link state ID (external network number).
Advertising Router	Advertising router's ID.
LS Seq Number	Link state sequence number (detects old or duplicate link state advertisements).
Checksum	LS checksum (Fletcher checksum of the complete contents of the LSA).
Length	Length in bytes of the link state advertisement.
Network Mask	Network mask implemented.
Metric Type	External Type.
TOS	Type of service.
Metric	Link state metric.
Forward Address	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.
External Route Tag	External route tag, a 32-bit field attached to each external route. This is not used by the OSPF protocol itself.

The following is sample output from the **showipospfdatabase**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 128: show ip ospf database network Field Descriptions

Field	Description
OSPF Router with id	Router ID number.
Process ID 300	OSPF process ID.

Field	Description
LS age	Link state age.
Options	Type of service options (Type 0 only).
LS Type:	Link state type.
Link State ID	Link state ID of designated router.
Advertising Router	Advertising router's ID.
LS Seq Number	Link state sequence (detects old or duplicate link state advertisements).
Checksum	LS checksum (Fletcher checksum of the complete contents of the link state advertisement).
Length	Length in bytes of the link state advertisement.
Network Mask	Network mask implemented.
AS Boundary Router	Definition of router type.
Attached Router	List of routers attached to the network, by IP address.

The following is sample output from the **showipospfdatabase**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 129: show ip ospf database router Field Descriptions

Field	Description
OSPF Router with id	Router ID number.
Process ID	OSPF process ID.
LS age	Link state age.

Field	Description
Options	Type of service options (Type 0 only).
LS Type	Link state type.
Link State ID	Link state ID.
Advertising Router	Advertising router's ID.
LS Seq Number	Link state sequence (detects old or duplicate link state advertisements).
Checksum	LS checksum (Fletcher checksum of the complete contents of the link state advertisement).
Length	Length in bytes of the link state advertisement.
AS Boundary Router	Definition of router type.
Number of Links	Number of active links.
link ID	Link type.
Link Data	Router interface address.
TOS	Type of service metric (Type 0 only).

The following is sample output from **showipospfdatabase**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 130: show ip ospf database summary Field Descriptions

Field	Description
OSPF Router with id	Router ID number.
Process ID	OSPF process ID.
LS age	Link state age.
Options	Type of service options (Type 0 only).
LS Type	Link state type.

Field	Description
Link State ID	Link state ID (summary network number).
Advertising Router	Advertising router's ID.
LS Seq Number	Link state sequence (detects old or duplicate link state advertisements).
Checksum	LS checksum (Fletcher checksum of the complete contents of the link state advertisement).
Length	Length in bytes of the link state advertisement.
Network Mask	Network mask implemented.
TOS	Type of service.
Metric	Link state metric.

The following is sample output from **showipospfdatabase**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        3        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 131: show ip ospf database database-summary Field Descriptions

Field	Description
Area 0 database summary	Area number.
Count	Count of LSAs of the type identified in the first column.

Field	Description
Router	Number of router link state advertisements in that area.
Network	Number of network link state advertisements in that area.
Summary Net	Number of summary link state advertisements in that area.
Summary ASBR	Number of summary autonomous system boundary router (ASBR) link state advertisements in that area.
Type-7 Ext	Type-7 LSA count.
Self-originated Type-7	Self-originated Type-7 LSA.
Opaque Link	Type-9 LSA count.
Opaque Area	Type-10 LSA count
Subtotal	Sum of LSAs for that area.
Delete	Number of link state advertisements that are marked “Deleted” in that area.
Maxage	Number of link state advertisements that are marked “Maxaged” in that area.
Process 1 database summary	Database summary for the process.
Count	Count of LSAs of the type identified in the first column.
Router	Number of router link state advertisements in that process.
Network	Number of network link state advertisements in that process.
Summary Net	Number of summary link state advertisements in that process.
Summary ASBR	Number of summary autonomous system boundary router (ASBR) link state advertisements in that process.
Type-7 Ext	Type-7 LSA count.
Opaque Link	Type-9 LSA count.
Opaque Area	Type-10 LSA count.
Type-5 Ext	Type-5 LSA count.
Self-Originated Type-5	Self-originated Type-5 LSA count.
Opaque AS	Type-11 LSA count.
Total	Sum of LSAs for that process.
Delete	Number of link state advertisements that are marked “Deleted” in that process.
Maxage	Number of link state advertisements that are marked “Maxaged” in that process.

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

process-id	(Optional) Process ID number. If this argument is included, only information for the specified routing process is included. The range is 1 to 65535.
type	(Optional) Interface type. If the *type* argument is included, only information for the specified interface type is included.
number	(Optional) Interface number. If the *number* argument is included, only information for the specified interface number is included.
brief	(Optional) Displays brief overview information for OSPF interfaces, states, addresses and masks, and areas on the device.
multicast	(Optional) Displays multicast information.
topology *topology-name*	(Optional) Displays OSPF-related information about the named topology instance.
topology base	(Optional) Displays OSPF-related information about the base topology.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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
```

```
  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)
```

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
```

.
.
.

The table below describes the significant fields shown in the displays.

*Table 132: **show ip ospf interface** Field Descriptions*

Field	Description
Ethernet	Status of the physical link and operational status of the protocol.
Process ID	OSPF process ID.
Area	OSPF area.
Cost	Administrative cost assigned to the interface.
State	Operational state of the interface.
Nbrs F/C	OSPF neighbor count.
Internet Address	Interface IP address, subnet mask, and area address.
Topology-MTID	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.
Transmit Delay	Transmit delay in seconds, interface state, and device priority.
Designated Router	Designated router ID and respective interface IP address.
Backup Designated router	Backup designated router ID and respective interface IP address.
Timer intervals configured	Configuration of timer intervals.
Hello	Number of seconds until the next hello packet is sent out this interface.
Strict TTL checking enabled	Only one hop is allowed.
Strict TTL checking enabled, up to 4 hops allowed	A set number of hops has been explicitly configured.
Neighbor Count	Count of network neighbors and list of adjacent neighbors.

show ip ospf neighbor

To display Open Shortest Path First (OSPF) neighbor information on a per-interface basis, use the **showipospfneighbor** command in privileged EXEC mode.

show ip ospf neighbor [*interface-type interface-number*] [*neighbor-id*] [**detail**] [**summary** [**per-instance**]]

Syntax Description

interface-type interface-number	(Optional) Type and number associated with a specific OSPF interface.
neighbor-id	(Optional) Neighbor hostname or IP address in A.B.C.D format.
detail	(Optional) Displays all neighbors given in detail (lists all neighbors).
summary	(Optional) Displays total number summary of all neighbors.
per-instance	(Optional) Displays total number of neighbors in each neighbor state. The output is printed for each configured OSPF instance separately.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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

   ID           Pri   State         Dead Time     Address         Interface
172.16.48.1      1    FULL/DROTHER  0:00:33    172.16.48.1       Fddi0
172.16.48.200    1    FULL/DROTHER  0:00:32    172.16.48.200     Fddi0
10.199.199.137   5    FULL/DR       0:00:32    172.16.48.189     Fddi0
```

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 133: show ip ospf neighbor detail Field Descriptions

Field	Description
Neighbor	Neighbor router ID.
interface address	IP address of the interface.
In the area	Area and interface through which the OSPF neighbor is known.
Neighbor priority	Router priority of the neighbor and neighbor state.
State	OSPF state. If one OSPF neighbor has enabled TTL security, the other side of the connection will show the neighbor in the INIT state.

Field	Description
state changes	Number of state changes since the neighbor was created. This value can be reset using the **clearipospfcountersneighbor** command.
DR is	Router ID of the designated router for the interface.
BDR is	Router ID of the backup designated router for the interface.
Options	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.)
LLS Options..., last OOB-Resync	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.
Dead timer due in	Expected time in hours:minutes:seconds before Cisco IOS software will declare the neighbor dead.
Neighbor is up for	Number of hours:minutes:seconds since the neighbor went into the two-way state.
Index	Neighbor location in the area-wide and autonomous system-wide retransmission queue.
retransmission queue length	Number of elements in the retransmission queue.
number of retransmission	Number of times update packets have been re-sent during flooding.
First	Memory location of the flooding details.
Next	Memory location of the flooding details.
Last retransmission scan length	Number of link state advertisements (LSAs) in the last retransmission packet.
maximum	Maximum number of LSAs sent in any retransmission packet.
Last retransmission scan time	Time taken to build the last retransmission packet.
maximum	Maximum time, in milliseconds, taken to build any retransmission packet.

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

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
172.16.1.201  1 INIT/DROTHER   00.00.35  10.1.1.201   Ethernet0/0
```

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
```

```
EXSTART      0
EXCHANGE     0
LOADING      0
FULL         1
Total count  1    (Undergoing NSF 0)


             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)
```

Table 134: ***show ip ospf neighbor summary*** *and* ***show ip ospf neighbor summary per-instance*** *Field Descriptions*

Field	Description
DOWN	No information (hellos) has been received from this neighbor, but hello packets can still be sent to the neighbor in this state.
ATTEMPT	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.
INIT	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.
2WAY	This state designates that bi-directional communication has been established between two routers.
EXSTART	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 active, and to decide upon the initial DD sequence number. Neighbor conversations in this state or greater are called adjacencies.
EXCHANGE	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 the active router which is explicitly acknowledged by the secondary router. 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.

Field	Description
LOADING	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.
FULL	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.

show ip ospf virtual-links

To display parameters and the current state of Open Shortest Path First (OSPF) virtual links, use the **showipospfvirtual-links** command in EXEC mode.

show ip ospf virtual-links

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The information displayed by the **showipospfvirtual-links** command is useful in debugging OSPF routing operations.

Examples

The following is sample output from the **showipospfvirtual-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 135: **show ip ospf virtual-links** Field Descriptions*

Field	Description
Virtual Link to router 192.168.101.2 is up	Specifies the OSPF neighbor, and if the link to that neighbor is up or down.
Transit area 0.0.0.1	The transit area through which the virtual link is formed.
via interface Ethernet0	The interface through which the virtual link is formed.
Cost of using 10	The cost of reaching the OSPF neighbor through the virtual link.
Transmit Delay is 1 sec	The transmit delay (in seconds) on the virtual link.
State POINT_TO_POINT	The state of the OSPF neighbor.
Timer intervals...	The various timer intervals configured for the link.
Hello due in 0:00:08	When the next hello is expected from the neighbor.
Adjacency State FULL	The adjacency state between the neighbors.

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 commandsummary-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

ip-address	Summary address designated for a range of addresses.
mask	IP subnet mask used for the summary route.
prefix	IP route prefix for the destination.
not-advertise	(Optional) Suppresses routes that match the specified prefix/mask pair. This keyword applies to OSPF only.
tag *tag*	(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.
nssa-only	(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.

Command Default

This command behavior is disabled by default.

Command Modes

Router configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

R outes 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

Command	Description
area range	Consolidates and summarizes routes at an area boundary.
ip ospf authentication-key	Assigns a password to be used by neighboring routers that are using the simple password authentication of OSPF.
ip ospf message-digest-key	Enables OSPF MD5 authentication.

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.

timers throttle spf *spf-start spf-hold spf-max-wait*
no timers throttle spf *spf-start spf-hold spf-max-wait*

Syntax Description

spf-start	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.
spf-hold	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.
spf-max-wait	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.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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.

```
router ospf 1
 router-id 10.10.10.2
```

```
 log-adjacency-changes
 timers throttle spf 5 1000 90000
 redistribute static subnets
 network 10.21.21.0 0.0.0.255 area 0
 network 10.22.22.0 0.0.0.255 area 00
```

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

Command	Description
ospfv3 network manet	Sets the network type to Mobile Ad Hoc Network (MANET).

PART X

Security

- Security, on page 1191

Security

- aaa accounting, on page 1194
- aaa accounting dot1x, on page 1197
- aaa accounting identity, on page 1199
- aaa authentication dot1x, on page 1201
- aaa new-model, on page 1202
- authentication host-mode, on page 1204
- authentication logging verbose, on page 1206
- authentication mac-move permit, on page 1207
- authentication priority, on page 1209
- authentication violation, on page 1211
- cisp enable, on page 1213
- cisp enable, on page 1214
- clear device-tracking database, on page 1215
- clear errdisable interface vlan, on page 1219
- clear mac address-table, on page 1220
- confidentiality-offset, on page 1222
- debug aaa dead-criteria transaction, on page 1223
- delay-protection, on page 1225
- deny (MAC access-list configuration), on page 1226
- device-role (IPv6 snooping), on page 1229
- device-role (IPv6 nd inspection), on page 1230
- device-tracking (interface config), on page 1231
- device-tracking (VLAN config), on page 1234
- device-tracking binding, on page 1237
- device-tracking logging, on page 1257
- device-tracking policy, on page 1261
- device-tracking tracking, on page 1274
- device-tracking upgrade-cli, on page 1278
- dot1x critical (global configuration), on page 1281
- dot1x logging verbose, on page 1282
- dot1x pae, on page 1283
- dot1x supplicant controlled transient, on page 1284
- dot1x supplicant force-multicast, on page 1285

- dot1x test eapol-capable, on page 1286
- dot1x test timeout, on page 1287
- dot1x timeout, on page 1288
- dtls, on page 1290
- enable password, on page 1292
- enable secret, on page 1294
- epm access-control open, on page 1297
- include-icv-indicator, on page 1298
- ip access-list, on page 1299
- ip access-list role-based, on page 1302
- ip admission, on page 1303
- ip admission name, on page 1304
- ip dhcp snooping database, on page 1306
- ip dhcp snooping information option format remote-id, on page 1308
- ip dhcp snooping verify no-relay-agent-address, on page 1309
- ip http access-class, on page 1310
- ip radius source-interface, on page 1312
- ip source binding, on page 1314
- ip ssh source-interface, on page 1315
- ip verify source, on page 1316
- ipv6 access-list, on page 1317
- ipv6 snooping policy, on page 1319
- key chain macsec, on page 1320
- key config-key password-encrypt, on page 1321
- key-server, on page 1323
- limit address-count, on page 1324
- mab logging verbose, on page 1325
- mab request format attribute 32, on page 1326
- macsec-cipher-suite, on page 1328
- macsec network-link, on page 1329
- match (access-map configuration), on page 1330
- mka pre-shared-key, on page 1332
- mka suppress syslogs sak-rekey, on page 1333
- password encryption aes, on page 1334
- permit (MAC access-list configuration), on page 1336
- protocol (IPv6 snooping), on page 1339
- radius server, on page 1340
- radius-server dead-criteria, on page 1342
- radius-server deadtime, on page 1344
- radius-server directed-request, on page 1346
- radius-server domain-stripping, on page 1348
- sak-rekey, on page 1352
- security level (IPv6 snooping), on page 1353
- send-secure-announcements, on page 1354
- server-private (RADIUS), on page 1355
- server-private (TACACS+), on page 1357

- show aaa clients, on page 1359
- show aaa command handler, on page 1360
- show aaa dead-criteria, on page 1361
- **show aaa local**, on page 1363
- show aaa servers, on page 1365
- show aaa sessions, on page 1366
- show authentication brief, on page 1367
- show authentication sessions, on page 1370
- show cisp, on page 1373
- show device-tracking capture-policy, on page 1375
- show device-tracking counters, on page 1377
- show device-tracking database, on page 1379
- show device-tracking events, on page 1384
- show device-tracking features, on page 1386
- show device-tracking messages, on page 1387
- show device-tracking policies, on page 1388
- show device-tracking policy, on page 1389
- show dot1x, on page 1390
- show eap pac peer, on page 1392
- show ip access-lists, on page 1393
- show ip dhcp snooping statistics, on page 1396
- show radius server-group, on page 1399
- show tech-support acl, on page 1401
- show tech-support identity, on page 1405
- show vlan access-map, on page 1414
- show vlan filter, on page 1415
- show vlan group, on page 1416
- ssci-based-on-sci, on page 1417
- switchport port-security aging, on page 1418
- switchport port-security mac-address, on page 1420
- switchport port-security maximum, on page 1423
- switchport port-security violation, on page 1425
- tacacs server, on page 1427
- tracking (IPv6 snooping), on page 1428
- trusted-port, on page 1430
- use-updated-eth-header, on page 1431
- username, on page 1432
- vlan access-map, on page 1437
- vlan dot1Q tag native, on page 1439
- vlan filter, on page 1440
- vlan group, on page 1441

aaa accounting

To enable authentication, authorization, and accounting (AAA) accounting of requested services for billing or security purposes when you use RADIUS or TACACS+, use the **aaa accounting** command in global configuration mode. To disable AAA accounting, use the **no** form of this command.

aaa accounting {**auth-proxy** | **system** | **network** | **exec** | **connections** | **commands** *level*} {**default** | *list-name*} {**start-stop** | **stop-only** | **none**} [**broadcast**] **group** *group-name*
no aaa accounting {**auth-proxy** | **system** | **network** | **exec** | **connections** | **commands** *level*} {**default** | *list-name*} {**start-stop** | **stop-only** | **none**} [**broadcast**] **group** *group-name*

Syntax Description

auth-proxy	Provides information about all authenticated-proxy user events.
system	Performs accounting for all system-level events not associated with users, such as reloads.
network	Runs accounting for all network-related service requests.
exec	Runs accounting for EXEC shell session. This keyword might return user profile information such as what is generated by the **autocommand** command.
connection	Provides information about all outbound connections made from the network access server.
commands *level*	Runs accounting for all commands at the specified privilege level. Valid privilege level entries are integers from 0 through 15.
default	Uses the listed accounting methods that follow this argument as the default list of methods for accounting services.
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 groupname	At least one of the keywords described in the AAA Accounting Methods table.

Command Default

AAA accounting is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Use the **aaa accounting** command to enable accounting and to create named method lists defining specific accounting methods on a per-line or per-interface basis.

Table 136: AAA Accounting Methods

Keyword	Description
group radius	Uses the list of all RADIUS servers for authentication as defined by the **aaa group server radius** command.
group tacacs+	Uses the list of all TACACS+ servers for authentication as defined by the **aaa group server tacacs+** command.
group *group-name*	Uses a subset of RADIUS or TACACS+ servers for accounting as defined by the server group group-name.

In 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.

Note System accounting does not use named accounting lists; you can only define the default list for system accounting.

For minimal accounting, include the **stop-only** keyword to send a stop record accounting notice at the end of the requested user process. For more accounting, you can include the **start-stop** keyword, so that RADIUS or TACACS+ sends a start accounting notice at the beginning of the requested process and a stop accounting

notice at the end of the process. Accounting is stored only on the RADIUS or TACACS+ server. The none keyword disables accounting services for the specified line or interface.

When AAA accounting is activated, the network access server monitors either RADIUS accounting attributes or TACACS+ AV pairs pertinent to the connection, depending on the security method you have implemented. The network access server reports these attributes as accounting records, which are then stored in an accounting log on the security server.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

This command requires access to a RADIUS server.

We recommend that you enter the **dot1x reauthentication** interface configuration command before configuring IEEE 802.1x RADIUS accounting on an interface.

This example shows how to configure IEEE 802.1x accounting:

```
Device> 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+**} [**group** {*name* | **radius** | **tacacs+**} **. . .**] }
no aaa accounting identity {*name* | **default** }

Syntax Description

name	Name of a server group. This is optional when you enter it after the **broadcast group** and **group** keywords.
default	Uses the accounting methods that follow as the default list for accounting services.
start-stop	Sends a start accounting notice at the beginning of a process and a stop accounting notice at the end of a process. The start accounting record is sent in the background. The requested-user process begins regardless of whether or not the start accounting notice was received by the accounting server.
broadcast	Enables accounting records to be sent to multiple AAA servers and send accounting records to the first server in each group. If the first server is unavailable, the switch uses the list of backup servers to identify the first server.
group	Specifies the server group to be used for accounting services. These are valid server group names: • *name* — Name of a server group. • **radius** — Lists of all RADIUS hosts. • **tacacs+** — Lists of all TACACS+ hosts. The **group** keyword is optional when you enter it after the **broadcast group** and **group** keywords. You can enter more than optional **group** keyword.
radius	(Optional) Enables RADIUS authorization.
tacacs+	(Optional) Enables TACACS+ accounting.

Command Default

AAA accounting is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

To enable AAA accounting identity, you need to enable policy mode. To enable policy mode, enter the **authentication display new-style** command in privileged EXEC mode.

This example shows how to configure IEEE 802.1x accounting identity:

```
Device# authentication display new-style

Please note that while you can revert to legacy style
configuration at any time unless you have explicitly
entered new-style configuration, the following caveats
should be carefully read and understood.

(1) If you save the config in this mode, it will be written
    to NVRAM in NEW-style config, and if you subsequently
    reload the router without reverting to legacy config and
    saving that, you will no longer be able to revert.

(2) In this and legacy mode, Webauth is not IPv6-capable. It
    will only become IPv6-capable once you have entered new-
    style config manually, or have reloaded with config saved
    in 'authentication display new' mode.

Device# configure terminal
Device(config)# aaa accounting identity default start-stop group radius
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

Release	Modification
Cisco IOS XE Fuji 16.9.2	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 new-model

To enable the authentication, authorization, and accounting (AAA) access control model, issue the **aaa new-model** command in global configuration mode. To disable the AAA access control model, use the **no** form of this command.

aaa new-model
no aaa new-model

Syntax Description

This command has no arguments or keywords.

Command Default

AAA is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

This command enables the AAA access control system.

If the **login local** command is configured for a virtual terminal line (VTY), and the **aaa new-model** command is removed, you must reload the switch to get the default configuration or the **login** command. If the switch is not reloaded, the switch defaults to the **login local** command under the VTY.

Note We do not recommend removing the **aaa new-model** command.

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

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.
aaa authentication arap	Enables an AAA authentication method for ARAP using TACACS+.
aaa authentication enable default	Enables AAA authentication to determine if a user can access the privileged command level.
aaa authentication login	Sets AAA authentication at login.
aaa authentication ppp	Specifies one or more AAA authentication method for use on serial interfaces running PPP.
aaa authorization	Sets parameters that restrict user access to a network.

authentication host-mode

To set the authorization manager mode on a port, use the **authentication host-mode** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

authentication host-mode {**multi-auth** | **multi-domain** | **multi-host** | **single-host**}
no authentication host-mode

Syntax Description

multi-auth	Enables multiple-authorization mode (multi-auth mode) on the port.
multi-domain	Enables multiple-domain mode on the port.
multi-host	Enables multiple-host mode on the port.
single-host	Enables single-host mode on the port.

Command Default

Single host mode is enabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Single-host mode should be configured if only one data host is connected. Do not connect a voice device to authenticate on a single-host port. Voice device authorization fails if no voice VLAN is configured on the port.

Multi-domain mode should be configured if data host is connected through an IP phone to the port. Multi-domain mode should be configured if the voice device needs to be authenticated.

Multi-auth mode should be configured to allow devices behind a hub to obtain secured port access through individual authentication. Only one voice device can be authenticated in this mode if a voice VLAN is configured.

Multi-host mode also offers port access for multiple hosts behind a hub, but multi-host mode gives unrestricted port access to the devices after the first user gets authenticated.

This example shows how to enable multi-auth mode on a port:

```
Device> 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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

This command filters details, such as anticipated success, from authentication system messages. Failure messages are not filtered.

To filter verbose authentication system messages:

```
Device> 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

Command	Description
authentication logging verbose	Filters details fro
dot1x logging verbose	Filters details fro
mab logging verbose	Filters details fro

authentication mac-move permit

To enable MAC move on a device, use the **authentication mac-move permit** command in global configuration mode. To disable MAC move, use the **no** form of this command.

authentication mac-move permit
no authentication mac-move permit

Syntax Description

This command has no arguments or keywords.

Command Default

MAC move is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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:

```
Device> enable
Device# configure terminal
Device(config)# authentication mac-move permit
Device(config)# exit
```

Related Commands

Command	Description
access-session mac-move deny	Disables MAC move on a device.
authentication event	Sets the action for specific authentication events
authentication fallback	Configures a port to use web authentication as a IEEE 802.1x authentication.
authentication host-mode	Sets the authorization manager mode on a port.
authentication open	Enables or disables open access on a port.
authentication order	Sets the order of authentication methods used or
authentication periodic	Enable or disables reauthentication on a port.
authentication port-control	Enables manual control of the port authorization

Command	Description
authentication priority	Adds an authentication method to the port-priority l
authentication timer	Configures the timeout and reauthentication parame
authentication violation	Configures the violation modes that occur when a n device connects to a port with the maximum numbe
show authentication	Displays information about authentication manager

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 authenti 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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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

Command	Description
authentication control-direction	Configures the port mode as unidirectional or bidirectional.
authentication event fail	Specifies how the Auth Manager handles authentication failures as a r
authentication event no-response action	Specifies how the Auth Manager handles authentication failures as a r
authentication event server alive action reinitialize	Reinitializes an authorized Auth Manager session when a previously u and accounting server becomes available.
authentication event server dead action authorize	Authorizes Auth Manager sessions when the authentication, authoriza unreachable.
authentication fallback	Enables a web authentication fallback method.
authentication host-mode	Allows hosts to gain access to a controlled port.
authentication open	Enables open access on a port.
authentication order	Specifies the order in which the Auth Manager attempts to authentica
authentication periodic	Enables automatic reauthentication on a port.
authentication port-control	Configures the authorization state of a controlled port.
authentication timer inactivity	Configures the time after which an inactive Auth Manager session is t
authentication timer reauthenticate	Specifies the period of time between which the Auth Manager attemp
authentication timer restart	Specifies the period of time after which the Auth Manager attempts to
authentication violation	Specifies the action to be taken when a security violation occurs on a
mab	Enables MAC authentication bypass on a port.
show authentication registrations	Displays information about the authentication methods that are registe
show authentication sessions	Displays information about current Auth Manager sessions.
show authentication sessions interface	Displays information about the Auth Manager for a given interface.

authentication violation

To configure the violation modes that occur when a new device connects to a port or when a new device connects to a port after the maximum number of devices are connected to that port, use the **authentication violation** command in interface configuration mode.

authentication violation { **protect** | **replace** | **restrict** | **shutdown** }
no authentication violation { **protect** | **replace** | **restrict** | **shutdown** }

Syntax Description

protect	Drops unexpected incoming MAC addresses. No syslog errors are generated.
replace	Removes the current session and initiates authentication with the new host.
restrict	Generates a syslog error when a violation error occurs.
shutdown	Error-disables the port or the virtual port on which an unexpected MAC address occurs.

Command Default

Authentication violation shutdown mode is enabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Use the **authentication violation** command to specify the action to be taken when a security violation occurs on a port.

This example shows how to configure an IEEE 802.1x-enabled port as error-disabled and to shut down when a new device connects it:

```
Device> 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 running-config interface** *interface-name* 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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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
```

Related Commands

Command	Description
dot1x credentials*profile*	Configures a profile on a supplicant device.
dot1x supplicant force-multicast	Forces 802.1X supplicant to send multicast pac
dot1x supplicant controlled transient	Configures controlled access by 802.1X suppli
show cisp	Displays CISP information for a specified inter

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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
```

Related Commands

Command	Description
dot1x credentials*profile*	Configures a profile on a supplicant device.
dot1x supplicant force-multicast	Forces 802.1X supplicant to send multicast packet
dot1x supplicant controlled transient	Configures controlled access by 802.1X supplican
show cisp	Displays CISP information for a specified interfac

clear device-tracking database

To delete device-tracking database (binding table) entries, and clear counters, events, and messages, enter the **clear device-tracking** command in privileged EXEC mode.

clear device-tracking { **counters** [**interface** *inteface_type_no* | **vlan** *vlan_id*] | **database** [**address** { *hostname* | **all** } [**interface** *inteface_type_no* | **policy** *policy_name* | **vlan** *vlan_id*] | **interface** *inteface_type_no* [**vlan** *vlan_id*] | **mac** *mac_address* [**interface** *inteface_type_no* | **policy** *policy_name* | **vlan** *vlan_id*] | **policy** *policy_name* | **prefix** { *prefix* | **all** } [**interface** *inteface_type_no* | **policy** *policy_name* | **vlan** *vlan_id*] | **vlanid** *vlan_id*] | **events** | **messages** }

Syntax Description

counters	Clears device-tracking counters for the specified interface or VLAN. Counters are displayed in the **show device-tracking counters all** privileged EXEC command.
interface *inteface_type_no*	Enter an interface type and number. Use the question mark (?) online help function to display the types of interfaces available on the device. The clear action is performed for the interface you specify.
vlan *vlan_id*	Enter a VLAN ID. The clear action is performed for the VLAN ID you specify. The valid value range is from 1 to 4095.
database	Clears dynamic entries in the binding table. **Note** Static entries configured by using the **device-tracking binding vlan** *vlan_id* command are not deleted. You can delete all the dynamic entries in the table, or optionally, you can specify one or more IP addresses, MAC addresses, IPv6 prefixes, entries on a particular interface or VLAN, or a policy.
hostname	Enter the hostname or IP address on which you want to perform the clear action.
all	Performs the clear action on all IP addresses or IPv6 prefixes.
policy *policy_name*	Performs the clear action on the specified policy. Enter the policy name.
mac *mac_address*	Performs the clear action on the specified MAC address. Enter the MAC address.
prefix *prefix*	Performs the clear action on the specified IPv6 prefix. Enter a prefix or enter **all** to indicate all prefixes.
events	Clears the device-tracking events history. Events are displayed in the **show device-tracking events** privileged EXEC command.
messages	Clears the device-tracking message history. Events are displayed in the **show device-tracking messages** privileged EXEC command.

Command Default

Database entries go through their binding entry lifecycle.

Counters: Each counter is a nonnegative 32-bit integer and it wraps-around when the limit is reached.

Events and messages: After the limit of 255 is reached, starting with the oldest, events and messages are overwritten.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Examples

The following example shows you how to clear all entries from the binding table.

```
Device# show device-tracking database Binding Table has 25 entries, 25 dynamic (limit 200000)
Codes: L - Local, S - Static, ND - Neighbor Discovery, ARP - Address Resolution Protocol,
DH4 - IPv4 DHCP, DH6 - IPv6 DHCP, PKT - Other Packet, API - API created
Preflevel flags (prlvl):
0001:MAC and LLA match     0002:Orig trunk            0004:Orig access
0008:Orig trusted trunk    0010:Orig trusted access   0020:DHCP assigned
0040:Cga authenticated     0080:Cert authenticated    0100:Statically assigned


    Network Layer Address                  Link Layer Address     Interface  vlan
prlvl      age        state      Time left
ARP 192.0.9.49                             001d.4411.3ab7         Te1/0/4    200
00FF       22s        REACHABLE  699 s
ARP 192.0.9.48                             001d.4411.3ab7         Te1/0/4    200
00FF       22s        REACHABLE  691 s
ARP 192.0.9.47                             001d.4411.3ab7         Te1/0/4    200
00FF       22s        REACHABLE  687 s
ARP 192.0.9.46                             001d.4411.3ab7         Te1/0/4    200
00FF       22s        REACHABLE  714 s
ARP 192.0.9.45                             001d.4411.3ab7         Te1/0/4    200
00FF       22s        REACHABLE  692 s
ARP 192.0.9.44                             001d.4411.3ab7         Te1/0/4    200
00FF       22s        REACHABLE  702 s
ARP 192.0.9.43                             001c.4411.3ab7         Te1/0/4    200
00FF       22s        REACHABLE  680 s
ARP 192.0.9.42                             001c.4411.3ab7         Te1/0/4    200
00FF       22s        REACHABLE  708 s
ARP 192.0.9.41                             001c.4411.3ab7         Te1/0/4    200
00FF       22s        REACHABLE  683 s
ARP 192.0.9.40                             001c.4411.3ab7         Te1/0/4    200
00FF       22s        REACHABLE  708 s
ARP 192.0.9.39                             001c.4411.3ab7         Te1/0/4    200
00FF       22s        REACHABLE  710 s
ARP 192.0.9.38                             001c.4411.3ab7         Te1/0/4    200
00FF       22s        REACHABLE  697 s
ARP 192.0.9.37                             001c.4411.3ab7         Te1/0/4    200
00FF       22s        REACHABLE  707 s
ARP 192.0.9.36                             001c.4411.3ab7         Te1/0/4    200
00FF       22s        REACHABLE  695 s
ARP 192.0.9.35                             001c.4411.3ab7         Te1/0/4    200
00FF       22s        REACHABLE  708 s
ARP 192.0.9.34                             001c.4411.3ab7         Te1/0/4    200
00FF       22s        REACHABLE  706 s
```

```
ARP 192.0.9.33                                  001b.4411.3ab7         Te1/0/4    200
00FF       22s        REACHABLE  683 s
ARP 192.0.9.32                                  001b.4411.3ab7         Te1/0/4    200
00FF       22s        REACHABLE  697 s
ARP 192.0.9.31                                  001b.4411.3ab7         Te1/0/4    200
00FF       22s        REACHABLE  683 s
ARP 192.0.9.30                                  001b.4411.3ab7         Te1/0/4    200
00FF       22s        REACHABLE  678 s
ARP 192.0.9.29                                  001b.4411.3ab7         Te1/0/4    200
00FF       22s        REACHABLE  696 s
ARP 192.0.9.28                                  001b.4411.3ab7         Te1/0/4    200
00FF       22s        REACHABLE  704 s
ARP 192.0.9.27                                  001b.4411.3ab7         Te1/0/4    200
00FF       22s        REACHABLE  713 s
ARP 192.0.9.26                                  001b.4411.3ab7         Te1/0/4    200
00FF       22s        REACHABLE  695 s
ARP 192.0.9.25                                  001b.4411.3ab7         Te1/0/4    200
00FF       22s        REACHABLE  686 s

Device# clear device-tracking database

*Dec 13 15:10:22.837: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.49 VLAN=200
MAC=001d.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:10:22.838: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.48 VLAN=200
MAC=001d.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:10:22.838: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.47 VLAN=200
MAC=001d.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:10:22.838: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.46 VLAN=200
MAC=001d.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:10:22.839: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.45 VLAN=200
MAC=001d.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:10:22.839: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.44 VLAN=200
MAC=001d.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:10:22.839: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.43 VLAN=200
MAC=001c.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:10:22.839: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.42 VLAN=200
MAC=001c.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:10:22.840: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.41 VLAN=200
MAC=001c.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:10:22.840: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.40 VLAN=200
MAC=001c.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:10:22.840: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.39 VLAN=200
MAC=001c.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:10:22.841: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.38 VLAN=200
MAC=001c.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:10:22.841: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.37 VLAN=200
MAC=001c.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:10:22.841: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.36 VLAN=200
MAC=001c.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:10:22.842: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.35 VLAN=200
MAC=001c.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:10:22.842: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.34 VLAN=200
MAC=001c.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:10:22.842: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.33 VLAN=200
MAC=001b.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:10:22.842: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.32 VLAN=200
MAC=001b.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:10:22.843: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.31 VLAN=200
MAC=001b.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:10:22.843: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.30 VLAN=200
MAC=001b.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:10:22.843: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.29 VLAN=200
MAC=001b.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:10:22.844: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.28 VLAN=200
```

```
MAC=001b.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:10:22.844: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.27 VLAN=200
MAC=001b.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:10:22.844: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.26 VLAN=200
MAC=001b.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:10:22.844: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.25 VLAN=200
MAC=001b.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF

Device# show device-tracking database
<no output; binding table cleared>
```

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. I

Command Default

No default behavior or values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

You can reenable a port by using the **shutdown** and **no shutdown** interface configuration commands, or you can clear error-disable for VLANs by using the **clear errdisable** interface command.

Examples

This example shows how to reenable all VLANs that were error-disabled on Gigabit Ethernet port 4/0/2:

```
Device# clear errdisable interface gigabitethernet4/0/2 vlan
```

Related Commands

Command	Description
errdisable detect cause	Enables error-disabled detectio
errdisable recovery	Configures the recovery mecha
show errdisable detect	Displays error-disabled detecti
show errdisable recovery	Displays error-disabled recover
show interfaces status err-disabled	Displays interface status of a li

clear mac address-table

To delete from the MAC address table a specific dynamic address, all dynamic addresses on a particular interface, all dynamic addresses on stack members, or all dynamic addresses on a particular VLAN, use the **clear mac address-table** command in privileged EXEC mode. This command also clears the MAC address notification global counters.

clear mac address-table {**dynamic** [**address** *mac-addr* | **interface** *interface-id* | **vlan** *vlan-id*] | **move update** | **notification**}

Syntax Description

dynamic	Deletes all dynamic MAC addresses.
address *mac-addr*	(Optional) Deletes the specified dynamic MAC address
interface *interface-id*	(Optional) Deletes all dynamic MAC addresses on the s
vlan *vlan-id*	(Optional) Deletes all dynamic MAC addresses for the s
move update	Clears the MAC address table move-update counters.
notification	Clears the notifications in the history table and reset the

Command Default

No default behavior or values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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
```

Related Commands

Command	Description
mac address-table notification	Enables the MAC address notification feature.
mac address-table move update {**receive** | **transmit**}	Configures MAC address-table move update on the device.
show mac address-table	Displays the MAC address table static and dynamic entries.
show mac address-table move update	Displays the MAC address-table move update information on the device.

Command	Description
show mac address-table notification	Displays the MAC address notification settings for all interfaces or on the specified interface when the **interface** keyword is appended.
snmp trap mac-notification change	Enables the SNMP MAC address notification trap on a specific interface.

confidentiality-offset

To enable MACsec Key Agreement protocol (MKA) to set the confidentiality offset for MACsec operations, use the **confidentiality-offset** command in MKA-policy configuration mode. To disable confidentiality offset, use the **no** form of this command.

confidentiality-offset
no confidentiality-offset

Syntax Description

This command has no arguments or keywords.

Command Default

Confidentiality offset is disabled.

Command Modes

MKA-policy configuration (config-mka-policy)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Examples

The following example shows how to enable the confidentiality offset:

```
Device> enable
Device# configure terminal
Device(config)# mka policy 2
Device(config-mka-policy)# confidentiality-offset
```

Related Commands

Command	Description
mka policy	Configures an MKA policy.
delay-protection	Configures MKA to use delay protection in sending MKPDU.
include-icv-indicator	Includes ICV indicator in MKPDU.
key-server	Configures MKA key-server options.
macsec-cipher-suite	Configures cipher suite for deriving SAK.
sak-rekey	Configures the SAK rekey interval.
send-secure-announcements	Configures MKA to send secure announcements in sending MKPDUs.
ssci-based-on-sci	Computes SSCI based on the SCI.
use-updated-eth-header	Uses the updated Ethernet header for ICV calculation.

debug aaa dead-criteria transaction

To display authentication, authorization, and accounting (AAA) dead-criteria transaction values, use the **debugaaadead-criteriatransaction**command in privileged EXEC mode. To disable dead-criteria debugging, use the **no** form of this command.

debug aaa dead-criteria transaction
no debug aaa dead-criteria transaction

Syntax Description

This command has no arguments or keywords.

Command Default

If the command is not configured, debugging is not turned on.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Dead-criteria transaction values may change with every AAA transaction. Some of the values that can be displayed are estimated outstanding transaction, retransmit tries, and dead-detect intervals. These values are explained in the table below.

Examples

The following example shows dead-criteria transaction information for a particular server group:

```
Device> enable
Device# debug aaa dead-criteria transaction

AAA Transaction debugs debugging is on
*Nov 14 23:44:17.403: AAA/SG/TRANSAC: Computed Retransmit Tries: 10, Current Tries: 3,
Current Max Tries: 10
*Nov 14 23:44:17.403: AAA/SG/TRANSAC: Computed Dead Detect Interval: 10s, Elapsed Time:
317s, Current Max Interval: 10s
*Nov 14 23:44:17.403: AAA/SG/TRANSAC: Estimated Outstanding Transaction: 6, Current Max
Transaction: 6
```

The table below describes the significant fields shown in the display.

Table 137: debug aaa dead-criteria transaction Field Descriptions

Field	Description
AAA/SG/TRANSAC	AAA server-group transaction.
Computed Retransmit Tries	Currently computed number of retransmissions before the server is marked as dead.
Current Tries	Number of successive failures since the last valid response.
Current Max Tries	Maximum number of tries since the last successful transaction.

Field	Description
Computed Dead Detect Interval	Period of inactivity (the number of seconds since the last successful transaction) that can elapse before the server is marked as dead. The period of inactivity starts when a transaction is sent to a server that is considered live. The dead-detect interval is the period that the device waits for responses from the server before the device marks the server as dead.
Elapsed Time	Amount of time that has elapsed since the last valid response.
Current Max Interval	Maximum period of inactivity since the last successful transaction.
Estimated Outstanding Transaction	Estimated number of transaction that are associated with the server.
Current Max Transaction	Maximum transaction since the last successful transaction.

Related Commands

Command	Description
radius-server dead-criteria	Forces one or both of the criteria, used to mark a RADIUS server as dead, to be the indicated constant.
show aaa dead-criteria	Displays dead-criteria detection information for an AAA server.

delay-protection

To configure MKA to use delay protection in sending MACsec Key Agreement Protocol Data Units (MKPDUs), use the **delay-protection** command in MKA-policy configuration mode. To disable delay protection, use the **no** form of this command.

delay-protection
no delay-protection

Syntax Description

This command has no arguments or keywords.

Command Default

Delay protection for sending MKPDUs is disabled.

Command Modes

MKA-policy configuration (config-mka-policy)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Examples

The following example shows how to configure MKA to use delay protection in sending MKPDUs:

```
Device> enable
Device# configure terminal
Device(config)# mka policy 2
Device(config-mka-policy)# delay-protection
```

Related Commands

Command	Description
mka policy	Configures an MKA policy.
confidentiality-offset	Sets the confidentiality offset for MACsec operations.
include-icv-indicator	Includes ICV indicator in MKPDU.
key-server	Configures MKA key-server options.
macsec-cipher-suite	Configures cipher suite for deriving SAK.
sak-rekey	Configures the SAK rekey interval.
send-secure-announcements	Configures MKA to send secure announcements in sending MKPDUs.
ssci-based-on-sci	Computes SSCI based on the SCI.
use-updated-eth-header	Uses the updated Ethernet header for ICV calculation.

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** | **lavc-sca** | **lsap** *lsap mask* | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** | **vines-ip** | **xns-idp**] [**cos** *cos*]
no deny {**any** | **host** *src-MAC-addr* | *src-MAC-addr mask*} {**any** | **host** *dst-MAC-addr* | *dst-MAC-addr mask*} [*type mask* | **aarp** | **amber** | **appletalk** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042** | **lat** | **lavc-sca** | **lsap** *lsap mask* | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** | **vines-ip** | **xns-idp**] [**cos** *cos*]

Syntax Description

any	Denies any source or destination MAC address.
host *src-MAC-addr* | *src-MAC-addr mask*	Defines a host MAC address and optional subnet matches the defined address, non-IP traffic from
host *dst-MAC-addr* | *dst-MAC-addr mask*	Defines a destination MAC address and optional a packet matches the defined address, non-IP traf
type mask	(Optional) Specifies the EtherType number of a pac to identify the protocol of the packet. The type is 0 to 65535, specified in hexadecimal. The mask is a mask of don't care bits applied to t
aarp	(Optional) Specifies EtherType AppleTalk Addres address to a network address.
amber	(Optional) Specifies EtherType DEC-Amber.
appletalk	(Optional) Specifies EtherType AppleTalk/EtherT
dec-spanning	(Optional) Specifies EtherType Digital Equipmen
decnet-iv	(Optional) Specifies EtherType DECnet Phase IV
diagnostic	(Optional) Specifies EtherType DEC-Diagnostic.
dsm	(Optional) Specifies EtherType DEC-DSM.
etype-6000	(Optional) Specifies EtherType 0x6000.
etype-8042	(Optional) Specifies EtherType 0x8042.
lat	(Optional) Specifies EtherType DEC-LAT.
lavc-sca	(Optional) Specifies EtherType DEC-LAVC-SCA

lsap *lsap-number mask*	(Optional) Specifies the LSAP number (0 to 6 identify the protocol of the packet. *mask* is a mask of don't care bits applied to th
mop-console	(Optional) Specifies EtherType DEC-MOP R
mop-dump	(Optional) Specifies EtherType DEC-MOP D
msdos	(Optional) Specifies EtherType DEC-MSDOS
mumps	(Optional) Specifies EtherType DEC-MUMP
netbios	(Optional) Specifies EtherType DEC- Networ
vines-echo	(Optional) Specifies EtherType Virtual Integra Banyan Systems.
vines-ip	(Optional) Specifies EtherType VINES IP.
xns-idp	(Optional) Specifies EtherType Xerox Netwo an arbitrary EtherType in decimal, hexadecim
cos *cos*	(Optional) Specifies a class of service (CoS) n CoS can be performed only in hardware. A war 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 extended configuration (config-ext-macl)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

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 138: IPX Filtering Criteria

IPX Encapsulation Type		Filter Criterion
Cisco IOS XE Name	**Novel Name**	
arpa	Ethernet II	EtherType 0x8137
snap	Ethernet-snap	EtherType 0x8137
sap	Ethernet 802.2	LSAP 0xE0E0
novell-ether	Ethernet 802.3	LSAP 0xFFFF

This example shows how to define the named MAC extended access list to deny NETBIOS traffic from any source to MAC address 00c0.00a0.03fa. Traffic matching this list is denied.

```
Device> 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.

Related Commands

Command	Description
mac access-list extended	Creates an access list based on MAC addresses for
permit	Permits from the MAC access-list configuration. Permits non-IP traffic to be forwarded if conditions
show access-lists	Displays access control lists configured on a device

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The **device-role** command specifies the role of the device attached to the port. By default, the device role is node.

The **switch** keyword indicates that the remote device is a switch and that the local switch is now operating in multiswitch mode; binding entries learned from the port will be marked with trunk_port preference level. If the port is configured as a trust-port, binding entries will be marked with trunk_trusted_port preference level.

This example shows how to define an IPv6 snooping policy name as policy1, place the device in IPv6 snooping configuration mode, and configure the device as the node:

```
Device> 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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The **device-role** command specifies the role of the device attached to the port. By default, the device role is host, and therefore all the inbound router advertisement and redirect messages are blocked.

The **switch** keyword indicates that the remote device is a switch and that the local switch is now operating in multiswitch mode; binding entries learned from the port will be marked with trunk_port preference level. If the port is configured as a trust-port, binding entries will be marked with trunk_trusted_port preference level.

The following example defines a Neighbor Discovery Protocol (NDP) policy name as policy1, places the device in ND inspection policy configuration mode, and configures the device as the host:

```
Device> 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 (interface config)

To enable SISF-based device tracking and attach the *default* policy to an interface or VLAN, or to enable the feature and attach a custom policy enter the **device-tracking** command in interface configuration mode. To detach the policy from the interface or VLAN and revert to default, use the **no** form of the command.

device-tracking [**attach-policy** *policy-name*] [**vlan** { *vlan-id* | **add** *vlan-id* | **all** | **except** *vlan-id* | **none** | **remove** *vlan-id* }]
no device-tracking [**attach-policy** *policy-name*] [**vlan** { *vlan-id* | **add** *vlan-id* | **all** | **except** *vlan-id* | **none** | **remove** *vlan-id* }]

Syntax Description

attach-policy *policy-name*	Attaches the custom policy that you specify, to the interface and all VLANs.
vlan { *vlan-id* | **add** *vlan-id* | **all** | **except** *vlan-id* | **none** | **remove** *vlan-id* }	Configures the VLAN list for the policy and attaches the custom policy to the specified VLANs. You can specify the following particulars: • *vlan-id*: Enter one or more VLAN IDs. The custom policy is attached to all the VLAN IDs. • **add***vlan-id*: Adds specified VLANs to the existing list of VLAN IDs. The custom policy is attached to all the VLAN IDs. • **all**: Attaches the custom policy to all VLAN IDs. This is the default option. • **except***vlan-id*: Attaches the custom policy to all VLAN IDs, except the ones you specify here. • **none**: Does not attach the custom policy to any VLAN. **remove***vlan-id*: Removes specified VLANs from the existing list of VLAN IDs. The custom policy is attached only to the VLAN IDs in the list.

Command Default

SISF-based device tracking is disabled and a policy is not attached to the interface.

Command Modes

Interface configuration [Device((config-if)#)]

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

If you enter the **device-tracking** command in the interface configuration mode, without any other keywords, the system attaches the *default* policy the interface or VLAN. The default policy is a built-in policy with default settings; you cannot change any of the attributes of the default policy.

If you configure the **device-tracking attach-policy***policy-name* command in the interface configuration mode, you can specify a custom policy name. You must have created the custom policy in global configuration mode already. The policy is attached to the specifed interface. You can then also specify the VLANs that you want to attach it to.

If you want to change the custom policy that is attached to a target, reconfigure the **device-tracking attach-policy***policy-name* command.

If you want to disable the feature on a particular target, enter the **no device-tracking** command in the interface configuration mode.

Examples

- Example: Enabling SISF-Based Device Tracking and Attaching the Default Policy, on page 1232
- Attaching a Custom Policy, on page 1232
- Example: Disabling SISF-Based Device-Tracking , on page 1233

Examples

The following example shows how to enable SISF-based device tracking and attach the default policy to an interface. The default policy has default policy parameters, none of which can be changed:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# interface tengigabitethernet1/0/1
Device(config-if)# device-tracking
Device(config-if)# end

Device# show device-tracking policies detail
Target               Type  Policy               Feature        Target range
Te1/0/1              PORT  default              Device-tracking vlan all
Te1/0/2              PORT  default              Device-tracking vlan all

Device-tracking policy default configuration:
  security-level guard
  device-role node
  gleaning from Neighbor Discovery
  gleaning from DHCP6
  gleaning from ARP
  gleaning from DHCP4
  NOT gleaning from protocol unkn
Policy default is applied on the following targets:
Target               Type  Policy               Feature        Target range
Te1/0/1              PORT  default              Device-tracking vlan all
Te1/0/2              PORT  default              Device-tracking vlan all
```

Examples

The following example shows how enable SISF-based device tracking and attach a custom policy called `sisf-01`, to the same interface as the above example, that is, `Te1/0/1`. Doing so replaces the existing default policy with custom policy `sisf-01` on `Te1/0/1`.

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# interface tengigabitethernet1/0/1
Device(config-if)# device-tracking attach-policy sisf-01
Device(config-if)# end

Device# show device-tracking policies detail
Target               Type  Policy               Feature        Target range
Te1/0/1              PORT  sisf-01              Device-tracking vlan all
Te1/0/2              PORT  default              Device-tracking vlan all

Device-tracking policy default configuration:
```

```
  security-level guard
  device-role node
  gleaning from Neighbor Discovery
  gleaning from DHCP6
  gleaning from ARP
  gleaning from DHCP4
  NOT gleaning from protocol unkn
Policy default is applied on the following targets:
Target              Type  Policy              Feature        Target range
Te1/0/2             PORT  default             Device-tracking vlan all
 Device-tracking policy sisf-01 configuration:
  security-level guard
  device-role node
  gleaning from Neighbor Discovery
  gleaning from DHCP6
  gleaning from ARP
  gleaning from DHCP4
  NOT gleaning from protocol unkn
  limit address-count 3000
Policy sisf-01 is applied on the following targets:
Target              Type  Policy              Feature        Target range
Te1/0/1             PORT  sisf-01             Device-tracking vlan all
```

Examples

The following example shows how to disable SISF-based device-tracking on a target. The feature is disabled on target Te1/0/1. This is the same interface where a custom policy is applied in the previous example. The default policy continues to be available on the other interface where the feature is enabled, that is, `Te1/0/2`.

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# interface tengigabitethernet1/0/1
Device(config-if)# no device-tracking attach-policy sisf-01
Device(config-if)# end

Device# show device-tracking policies detail
Target              Type  Policy              Feature        Target range
Te1/0/2             PORT  default             Device-tracking vlan all

Device-tracking policy default configuration:
  security-level guard
  device-role node
  gleaning from Neighbor Discovery
  gleaning from DHCP6
  gleaning from ARP
  gleaning from DHCP4
  NOT gleaning from protocol unkn
Policy default is applied on the following targets:
Target              Type  Policy              Feature        Target range
Te1/0/2             PORT  default             Device-tracking vlan all
```

device-tracking (VLAN config)

To enable Switch Integrated Security Features (SISF)-based device tracking and attach the *default* policy to a VLAN, or to enable the feature, attach a custom policy to a VLAN, and specify policy priority, enter the **device-tracking** command in VLAN configuration mode. To detach the policy from a VLAN and revert to default, use the **no** form of the command.

device-tracking [**attach-policy** *policy-name*] [**priority** *priority-value*]

Syntax Description

attach-policy *policy-name*		Attaches the custom policy that you specify, to the VLAN.
priority *priority-value*	**Note**	Although visible on the CLI, configuring this command has no effect. Policy priority is system-determined. You cannot change this.

Command Default

SISF-based device tracking is disabled.

Command Modes

VLAN configuration mode [Device((config-vlan-config)#)]

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced

Usage Guidelines

If you enter the **device-tracking** command in VLAN configuration mode, without any other keywords, the system attaches the *default* policy to the VLAN. The default policy is a built-in policy with default settings; you cannot change any of the parameters of the default policy.

If you configure the **device-tracking attach-policy***policy-name* command in VLAN configuration mode, the custom policy you specify is attached to the VLAN. With a custom policy, you can configure certain parameters of a custom policy.

You can enable the feature and attach a policy - custom or default - to one or more VLANs or a range of VLANs.

Examples

- Example: Enabling SISF-Based Device Tracking and Attaching the Default Policy, on page 1234
- Example: Attaching a Custom Policy to a VLAN, on page 1235
- Example: Attaching a Custom Policy to a Range of VLANs, on page 1235

Examples

The following example shows how to enable SISF-based device tracking and attach the default policy to VLAN 500:

```
Device# show device-tracking policies
Target               Type  Policy              Feature        Target range
Te1/0/1              PORT  sisf-03             Device-tracking vlan all
```

```
Te1/0/1             PORT  default             Address Resolution Relay vlan all
Te1/0/2             PORT  default             Device-tracking vlan all
vlan 333            VLAN  sisf-01             Device-tracking vlan all


Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#vlan configuration 500
Device(config-vlan-config)# device-tracking
Device(config-vlan-config)# end


Device#show device-tracking policies
Target              Type  Policy              Feature        Target range
Te1/0/1             PORT  sisf-03             Device-tracking vlan all
Te1/0/1             PORT  default             Address Resolution Relay vlan all
Te1/0/2             PORT  default             Device-tracking vlan all
vlan 333            VLAN  sisf-01             Device-tracking vlan allvlan 500
   VLAN  default              Device-tracking vlan all
```

Examples

The following example shows how to attach a custom policy called sisf-03, to the same VLAN as the above example, that is, VLAN 500. Doing so replaces the existing default policy with custom policy sisf-03 on the VLAN:

```
Device# show device-tracking policies
Target              Type  Policy              Feature        Target range
Te1/0/1             PORT  sisf-03             Device-tracking vlan all
Te1/0/1             PORT  default             Address Resolution Relay vlan all
Te1/0/2             PORT  default             Device-tracking vlan all
vlan 333            VLAN  sisf-01             Device-tracking vlan all
vlan 500            VLAN  default             Device-tracking vlan all

Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# vlan configuration 500
Device(config-vlan-config)# device-tracking attach-policy sisf-03
Device(config-vlan-config)# end

Device# show device-tracking policies
Target              Type  Policy              Feature        Target range
Te1/0/1             PORT  sisf-03             Device-tracking vlan all
Te1/0/1             PORT  default             Address Resolution Relay vlan all
Te1/0/2             PORT  default             Device-tracking vlan all
vlan 333            VLAN  sisf-01             Device-tracking vlan allvlan 500
   VLAN  sisf-03              Device-tracking vlan all
```

Examples

The following example shows how to attach a custom policy to a range of VLANs (VLANs 10 to 15):

```
Device(config)# vlan configuration 10-15
Device(config-vlan-config)#device-tracking attach-policy sisf-01
Device(config-vlan-config)#end

Device# show device-tracking policies
Target              Type  Policy              Feature        Target range
Te1/0/2             PORT  default             Device-tracking vlan all
vlan 10             VLAN  sisf-01             Device-tracking vlan all
vlan 11             VLAN  sisf-01             Device-tracking vlan all
vlan 12             VLAN  sisf-01             Device-tracking vlan all
vlan 13             VLAN  sisf-01             Device-tracking vlan all
```

```
vlan 14             VLAN  sisf-01             Device-tracking vlan all
vlan 15             VLAN  sisf-01             Device-tracking vlan all
```

device-tracking binding

To specify how binding entries are maintained in the binding table, enter the **device-tracking binding** command in global configuration mode. With this command you can configure the lifetime of each state, the maximum number of entries allowed in a binding table, and whether binding entry events are logged. You can also use this command to configure static binding entries. To revert to the default value, use the **no** form of the command.

device-tracking binding { **down-lifetime** | **logging** | **max-entries** | **reachable-lifetime** | **stale-lifetime** | **vlan** }

For the sake of clarity, the remaining command string after each one of the above options is listed separately:

- **device-tracking binding down-lifetime** { *seconds* | **infinite** }

  no device-tracking binding down-lifetime

- **device-tracking binding logging**

  no device-tracking binding logging

- **device-tracking binding max-entries** *no_of_entries* [**mac-limit** *no_of_entries* | **port-limit** *no_of_entries* [**mac-limit** *no_of_entries*] | **vlan-limit** *no_of_entries* [**mac-limit** *no_of_entries* | **port-limit** *no_of_entries* [**mac-limit** *no_of_entries*]]]

  no device-tracking binding max-entries

- **device-tracking binding reachable-lifetime** { *seconds* | **infinite** } [**down-lifetime** { *seconds* | **infinite** } | **stale-lifetime** { *seconds* | **infinite** } [**down-lifetime** { *seconds* | **infinite** }]]

  no device-tracking binding reachable-lifetime

- **device-tracking binding stale-lifetime** { *seconds* | **infinite** } [**down-lifetime** { *seconds* | **infinite** }]

  no device-tracking binding stale-lifetime

- **device-tracking binding vlan** *vlan_id* { *ipv4_add ipv6_add ipv6_prefix* } [**interface** *inteface_type_no*] [*48-bit-hardware-address*] [**reachable-lifetime** { *seconds* | **default** | **infinite** } **tracking** { **default** | **disable** | **enable** } **reachable-lifetime** { *seconds* | **default** | **infinite** }]

  no device-tracking binding vlan *vlan_id* { *ipv4_add ipv6_add ipv6_prefix* } [**interface** *inteface_type_no*] [*48-bit-hardware-address*] [**reachable-lifetime** { *seconds* | **default** | **infinite** } **tracking** { **default** | **disable** | **enable** } **reachable-lifetime** { *seconds* | **default** | **infinite** }]

Syntax Description

down-lifetime { *seconds* | **infinite** }	Provides the option to configure a countdown timer for a binding entry in the DOWN state, or, to disable the timer. A binding entry enters the DOWN state when the host's connecting interface is administratively down. If a timer is configured, one of these events may occur before timer expiry - either the interface can be up again, or, the entry can *remain* in the DOWN state. If the interface is up before timer expiry, the timer is stopped, and the state of the entry changes. If the entry remains in the DOWN state after timer expiry, it is removed from the binding table. If the timer is disabled or turned off, the entry is never removed from the binding table and can remain in the DOWN state indefinitely, or until the interface is up again. Configure one of these options: • *seconds*: Configure a value for the down-lifetime timer. Enter a value between 1 and 86400 seconds. The default value is 86400 seconds (24 hours). • **infinite**: Disables the timer for the DOWN state. This means that a timer is not started when an entry enters the DOWN state.
logging	Enables generation of logs for binding entry events.
device-tracking binding max-entries *no_of_entries* [**mac-limit** *no_of_entries* | **port-limit** *no_of_entries* | **vlan-limit** *no_of_entries*]	Configures the maximum number of entries for a binding table. Enter a value between 1 and 200000. The default value is 200000. **Note** This limit applies only to dynamic entries and not static binding entries. Optionally, you can also configure these limits: • **mac-limit** *no_of_entries*: Configures the maximum number of entries allowed per MAC address. Enter a value between 1 and 100000. By default, a limit is not set. • **port-limit** *no_of_entries*Configures the maximum number of entries allowed per interface. Enter a value between 1 and 100000. By default, a limit is not set. • **vlan-limit** *no_of_entries*: Configures the maximum number of entries allowed per VLAN. Enter a value between 1 and 100000. By default, a limit is not set. The **no** form of the command resets the **max-entries** value to 200000 and sets the **mac-limit**, **port-limit**, **vlan-limit** to "no limit".

reachable-lifetime { *seconds* | **infinite** }	Provides the option to configure a countdown timer for a binding entry in the REACHABLE state, or, to disable the timer. If a timer is configured, either one of these events may occur before timer expiry - incoming packets are received from the host, or there are no incoming packets from the host. Every time an incoming packet is received from the host, the timer is reset. If no incoming packets are received and the timer expires, then the state of the entry changes based on the reachability of the host. If the timer is disabled or turned off, the entry can remain in the REACHABLE state, indefinitely. Configure one of these options: • *seconds*: Configure a value for the reachable-lifetime timer. Enter a value between 1 and 86400 seconds. The default value is 300 seconds (5 minutes). • **infinite**: Disables the timer for the REACHABLE state. This means that a timer is not started when an entry enters the REACHABLE state.
stale-lifetime { *seconds* | **infinite** }	Provides the option to configure a countdown timer for a binding entry in the STALE state, or, to disable the timer. If a timer is configured, either one of these events may occur before timer expiry - incoming packets are received from the host, or there are no incoming packets from the host. If an incoming packet is received, the timer is stopped and the entry transitions to a new state. If no incoming packets are received and the timer expires, then the entry is removed from the binding table. If the timer is disabled or turned off, the entry can remain in the STALE state, indefinitely. If polling is enabled, a final attempt is made to probe the host at stale timer expiry. **Note** If polling is enabled, polling occurs when the reachable lifetime timer expires (3 times), and then a final attempt at stale timer expiry as well. The time required to poll an entry after expiry of reachable lifetime, is subtracted from the stale lifetime. Configure one of these options: • *seconds*: Configure a value for the stale-lifetime timer. Enter a value between 1 and 86400 seconds. The default value is 86400 seconds (24 hours). • **infinite**: Disables the timer for the STALE state. This means that a timer is not started when an entry enters the STALE state.

device-tracking binding vlan *vlan_id* { *ipv4_add ipv6_add ipv6_prefix* } { **interface** *inteface_type_no* } [*48-bit-hardware-address*] [**reachable-lifetime** { *seconds* | **default** | **infinite** } **tracking** { **default** | **disable** | **enable** } **reachable-lifetime** { *seconds* | **default** | **infinite** }]	Creates a static binding entry in the binding table. You can also specify how static binding entries are maintained in the binding table.
	Note The limit you configure for the **max-entries** *no_of_entries* option (above) does not apply to static binding entires. There is no limit to the number of static entries you can create.
	• Enter an IP address or prefix:
	  • *ipv4_add* : Enter an IPv4 address.
	  • *ipv6_add* : Enter an IPv6 address.
	  • *ipv6_prefix* : Enter an IPv6 prefix.
	• **interface** *inteface_type_no*: Enter an interface type and number. Use the question mark (?) online help function to display the types of interfaces available on the device.
	• (Optional) *48-bit-hardware-address*: Enter a MAC address. If you do not configure a MAC address for the binding entry, any MAC address is allowed.
	• (Optional) **reachable-lifetime** {*seconds* | **default** | **infinite** }: Configures the reachable lifetime settings for a static binding entry in the REACHABLE state. If you want to configure a reachable lifetime for a static binding entry, you must specify the MAC address for the entry.
	If you do not configure a value, the same value as configured for **device-tracking binding reachable-lifetime** applies.
	seconds: Configure a value for the reachable-lifetime timer. Enter a value between 1 and 86400 seconds. The default value is 300 seconds (5 minutes).
	default: Uses the same value as configured for dynamic entries in the binding table.
	infinite: Disables the timer for the REACHABLE state. This means that a timer is not started when a static binding entry enters the REACHABLE state.
	• (Optional) **tracking** {**default** | **disable** | **enable**}: Configures polling related settings for a static binding entry.
	default:Polling is disabled.
	disable: Disables polling for a static binding entry.
	enable: Enables polling for a static binding entry.

Command Default

If you do not configure a value, the default values for down, reachable, and stale lifetimes, and maximum number of binding entries allowed in a binding table are applicable - as long as a policy-level value is not set. See the *Usage Guidelines* below for further details.

Command Modes

Global configuration [Device(config)#]

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The **device-tracking binding** command enables you to specify how entries are maintained in a binding table, at a global level. The settings therefore apply to all interfaces and VLANs where SISF-based device-tracking is enabled. But for the system to start extracting binding information from packets that enter the network and to create binding entries to which the settings you configure here will apply, there must exist a policy that is attached an interface or VLAN.

If there is no policy on any interface or VLAN, the only entries that can exist in a binding table are any static binding entries you create.

Changing Any Binding Entry Setting

When you reconfigure a value or setting with the **device-tracking binding** command, the change applies only to subsequently created binding entries. The changed configuration does not apply to existing entries. The older setting applies to an older entry.

To display the current settings, enter the **show device-tracking database** command in privileged EXEC mode.

Global versus Policy-Level Settings

For some of the settings you configure with this command, there are policy level counterparts. (A policy level paramter is configured in the device-tracking configuration mode and applies only to that policy). The tables below clarifies when a globally configured value takes precedence and when a policy-level value takes precedence:

Option under device-tracking binding global configuration command	Policy-level counterpart in the device-tracking configuration mode
device-tracking binding reachable-lifetime { *seconds* | **infinite** }	**tracking enable** [**reachable-lifetime** [*seconds* | **infinite**]]

`Device(config)# device-tracking binding reachable-lifetime 2000`	`Device(config)# device-tracking policy sisf-01`
	`Device(config-device-tracking)#`
	`Device(config-device-tracking)# tracking enable`
	
	`reachable-lifetime 250`

If a policy-level value *and* a globally configured value exists, the policy-level value applies. If only a globally configured value exists, the globally configured value applies. If only a policy-level value exists the policy-level value applies. See: Example: Configuring a Reachable, Stale, and Down Lifetime at the Global vs Policy Level, on page 1245.	

Option under device-tracking binding global configuration command	Policy-level counterpart in the device-tracking configuration mode
device-tracking binding stale-lifetime { *seconds* | **infinite** }	**tracking disable** [**stale-lifetime** [*seconds* | **infinite**]]

Option under device-tracking binding global configuration command	Policy-level counterpart in the device-tracking configuration mode

`Device(config)# device-tracking binding stale-lifetime 2000`	`Device(config)# device-tracking policy sisf-01`
	`Device(config-device-tracking)#`
	`Device(config-device-tracking)# tracking enable`
	
	`stale-lifetime 500`

If a policy-level value *and* a globally configured value exists, the policy-level value applies. If only a globally configured value exists, the globally configured value applies. If only a policy-level value exists the policy-level value applies. See: Example: Configuring a Reachable, Stale, and Down Lifetime at the Global vs Policy Level, on page 1245.	

Option under device-tracking binding global configuration command	Policy-level counterpart in the device-tracking configuration mode
device-tracking binding max-entries *no_of_entries* [**mac-limit** *no_of_entries* | **port-limit** *no_of_entries* | **vlan-limit** *no_of_entries*]	**limit address-count***ip-per-port*

`Device(config)# device-tracking binding max-entries 30 vlan-limit 25 port-limit 20 mac-limit 19`	`Device(config)# device-tracking policy sisf-01`
	`Device(config-device-tracking)#`
	`Device(config-device-tracking)# limit address-count 30`

If a policy-level value *and* globally configured values exist, the creation of binding entries is stopped when a limit is reached - this can be one of the global values or the policy-level value. If only globally configured values exist, the creation of binding entries is stopped when a limit is reached. If only a policy-level value exists, the creation of binding entries is stopped when the policy-level limit is reached. Example: Global vs Policy-Level Address Limits, on page 1249.	

Option under device-tracking binding global configuration command	Policy-level counterpart in the device-tracking configuration mode
device-tracking binding max-entries *no_of_entries* [**mac-limit** *no_of_entries*]	IPv4 per MAC and IPv6 per MAC While you cannot configure either one of the above limits in a policy, a programmatically created policy may have either one, both, or neither one of the limits.

Option under device-tracking binding global configuration command	Policy-level counterpart in the device-tracking configuration mode

`Device(config)# device-tracking binding max-entries 300`
`mac-limit 3`
	`Device# show device-tracking policy LISP-DT-GLEAN-VLAN`
	
	`Policy LISP-DT-GLEAN-VLAN configuration:`
	`  security-level glean (*)`
	`  device-role node`
	`  gleaning from Neighbor Discovery`
	`  gleaning from DHCP`
	`  gleaning from ARP`
	`  gleaning from DHCP4`
	`  NOT gleaning from protocol unkn`
	`  limit address-count for IPv4 per mac 4 (*)`
	`  limit address-count for IPv6 per mac 12 (*)`
	`  tracking enable`
	`<output truncated>`

If a policy-level value *and* globally configured values exists, the creation of binding entries is stopped when a limit is reached - this can be one of the global values or the policy-level value. If only globally configured values exist, the creation of binding entries is stopped when a limit is reached. If only a policy-level value exists, the creation of binding entries is stopped when the policy-level limit is reached.	

Configuring Down, Reachable, Stale Lifetimes

When you configure a non-default value for the **down-lifetime**, or **reachable-lifetime**, or **stale-lifetime** keywords, the system reverts the lifetimes that you do not configure, to default values. The following example clarifies this behaviour: Example: Configuring Non-Default Values for Reachable, Stale, and Down Lifetimes, on page 1245.

To display the currently configured lifetime values, enter the **show running-config | include device-tracking** command in privileged EXEC mode.

Configuring MAC, Port, VLAN Limits

When you configure a non-default value for the **mac-limit**, or **port-limit**, or **vlan-limit** keywords, the system reverts the limits that you do not configure, to default values.

To configure all three limits in the same command line, first configure the VLAN limit, then the port limit, and finally the MAC limit:

```
Device(config)# device-tracking binding max-entries 15 vlan-limit 2 port-limit 20 mac-limit
 5
```

You can also use this system behavior when you want to reset one or more - but not *all* limits, to their default values. Although the default for all three keywords is that there is no limit, you cannot enter the number "0" to set a limit to its default value. Zero is not within the valid value range for any of the limits. To reset one or more limits to their default values, leave out the corresponding keyword. The following example clarifies this behaviour: Example: Setting VLAN, Port, and MAC Limits to Default Values, on page 1253.

Enabling Logging of Binding Entry Events

When you configure the **device-tracking binding logging** global configuration command to generate logs for binding entry events, you may also have to configure a few general logging settings, depending on your requirements:

- (Required) The **logging buffered informational** command in global configuration mode.

With this command you enable message logging at a device level and you specify a severity level. Configuring the command allows logs to be copied and stored to a local, internal buffer. Specifying a severity level causes messages at that level and numerically lower levels to be logged.

Logs generated for binding entry events have a severity level of 6 (meaning, informational). For example:

```
%SISF-6-ENTRY_CREATED: Entry created IP=192.0.2.24 VLAN=200 MAC=001b.4411.4ab6 I/F=Te1/0/4
Preflevel=00FF
```

- (Optional) The **logging console** command in global configuration mode.

  With this command you send the logs to the console (all available TTY lines).

Caution A low severity level may cause the number of messages being displayed on the console to increase significantly. Further, the console is a slow display device. In message storms some logging messages may be silently dropped when the console queue becomes full. Set severity levels accordingly.

If you don't want to configure this command, you can view logs when required by entering the **show logging** command in privileged EXEC mode.

If the **logging console** command is not enabled, logs are not *displayed* on the device console, but if you have configured **device-tracking binding logging** and **logging buffered informational**, logs will be generated and available in the local buffer.

For information about the *kind* of binding entry events for which logs are generated, see the system message guide for the corresponding release: System Message Guides. Search for `SISF-6`.

While the **device-tracking binding logging** command logs binding entry events, there is also the **device-tracking logging** command, which enables snooping security logging. The two command log different kinds of events and the generated logs have different severity levels.

Creating a Static Binding Entry

If there are silent but reachable hosts in the Layer 2 domain, and you want to retain binding information for these silent hosts, you can create static binding entries.

While there is no limit to the number of static entries you can create, these entries also contribute to the size of the binding table. Consider the number of such entries you require, before you create them.

You can create a static binding entry even if a policy is not attached to the interface or VLAN specified in the static binding entry.

When you configure a static binding entry followed by its settings (for example, reachable-lifetime), the configuration applies only to that static binding entry and not to any other entries, static or dynamic. The following example shows you how to created a static binding entry: Example: Creating a Static Binding Entry, on page 1248.

Examples

- Example: Configuring Non-Default Values for Reachable, Stale, and Down Lifetimes, on page 1245
- Example: Configuring a Reachable, Stale, and Down Lifetime at the Global vs Policy Level, on page 1245

- Example: Creating a Static Binding Entry, on page 1248
- Example: Global vs Policy-Level Address Limits, on page 1249
- Example: Setting VLAN, Port, and MAC Limits to Default Values, on page 1253
- Example: Global vs Policy-Level Limits Relating to MAC Addresses, on page 1254

Example: Configuring Non-Default Values for Reachable, Stale, and Down Lifetimes

The following example clarifies system behaviour when you configure values for reachable, stale, and down lifetimes seperately (the effect is not cumulative). It also show you how to configure values in a way that configuration is retained for all the lifetimes.

In the first step of this example only a reachable-lifetime is configured. This means the down-lifetime and stale lifetime are set to default, because the **stale-lifetime** and **down-lifetime** keywords have been left out:

```
Device(config)# device-tracking binding reachable-lifetime 700
Device(config)# exit
Device# show running-config | include device-tracking
device-tracking policy sisf-01
 device-tracking attach-policy sisf-01
 device-tracking attach-policy sisf-01 vlan 200device-tracking binding reachable-lifetime
700
device-tracking binding logging
```

In the next step of this example, a stale-lifetime of 1500 seconds and a down-lifetime of 1000 seconds is configured. With this, the reachable-lifetime configured in the previous step, is to default:

```
Device(config)# device-tracking binding stale-lifetime 1500 down-lifetime 1000
Device(config)# exit
Device# show running-config | include device-tracking
device-tracking policy sisf-01
 device-tracking attach-policy sisf-01
 device-tracking attach-policy sisf-01 vlan 200device-tracking binding stale-lifetime 1500
 down-lifetime 1000
device-tracking binding logging
```

In the next step of this example, reachable, down, and stale lifetimes of 700, 1000, and 200 respectively, are configured. With this, the value for the stale-lifetime is changed from 1500 seconds, to 1000 seconds. The down-lifetime is changed from 1000 to 200. The reachable-lifetime is configured as 700 seconds.

```
Device(config)# device-tracking binding reachable-lifetime 700 stale-lifetime 1000
down-lifetime 200
Device(config)# exit
Device# show running-config | include device-tracking
device-tracking policy sisf-01
 device-tracking attach-policy sisf-01
 device-tracking attach-policy sisf-01 vlan 200device-tracking binding reachable-lifetime
700 stale-lifetime 1000 down-lifetime 200
device-tracking binding logging
```

If any one of the lifetimes requires a change and the values for the other lifetimes must be retained, all three keywords must be reconfigured with the required values - everytime, and in the same command line.

Example: Configuring a Reachable, Stale, and Down Lifetime at the Global vs Policy Level

The following example shows you how to configure the reachable, stale, and down lifetimes for binding entries, at a global level. This example also shows you how you can then override the global setting and

configure a different lifetime for entries learnt on a particular interface or VLAN, by configuring a policy-level setting.

In the first part of the example, the output of the **show device-tracking policy** *policy-name* command shows that a policy-level value is not set and the default binding table settings are applicable to the existing entries. After a reachable, stale, and down lifetime is configured with the **device-tracking binding** command in global configuration mode, the new values are effective and are applied only to the four new entries that are added to the table.

Note In the output of the **show device-tracking database** command, note the `Time left` column for the binding entries. There is minor difference in the reachable lifetime of each entry. This is a system-imposed jitter (+/- 5 percent of the configured value), to ensure that system performance is not affected when a large number of entries are added to the binding table. Binding entries go through their lifecycle in a staggered manner thus preventing points of congestion.

Current configuration, which shows that policy-level reachable lifetime is not configured. The binding table entries show that the current reachable lifetime is 500 seconds (time left + age):

```
Device# show device-tracking policy sisf-01
Device-tracking policy sisf-01 configuration:
  security-level guard
  device-role node
  gleaning from Neighbor Discovery
  gleaning from DHCP6
  gleaning from ARP
  gleaning from DHCP4
  NOT gleaning from protocol unkn
Policy sisf-01 is applied on the following targets:
Target               Type  Policy               Feature        Target range
Te1/0/4              PORT  sisf-01              Device-tracking vlan 200

Device# show device-tracking database
Binding Table has 4 entries, 4 dynamic (limit 200000)
Codes: L - Local, S - Static, ND - Neighbor Discovery, ARP - Address Resolution Protocol,
DH4 - IPv4 DHCP, DH6 - IPv6 DHCP, PKT - Other Packet, API - API created
Preflevel flags (prlvl):
0001:MAC and LLA match     0002:Orig trunk            0004:Orig access
0008:Orig trusted trunk    0010:Orig trusted access   0020:DHCP assigned
0040:Cga authenticated     0080:Cert authenticated    0100:Statically assigned

Network Layer Address                          Link Layer Address     Interface  vlan
prlvl      age        state      Time left       <<<<
ARP 192.0.9.9                                  000a.959d.6816         Te1/0/4    200
0064       40s        REACHABLE  466 s
ARP 192.0.9.8                                  000a.959d.6816         Te1/0/4    200
0064       40s        REACHABLE  472 s
ARP 192.0.9.7                                  000a.959d.6816         Te1/0/4    200
0064       40s        REACHABLE  470 s
ARP 192.0.9.6                                  000a.959d.6816         Te1/0/4    200
0064       40s        REACHABLE  469 s
```

Configuration of reachable, stale and down lifetime at the global level. New values apply only to binding entries created after this:

```
Device(config)# device-tracking binding reachable-lifetime 700 stale-lifetime 1000
down-lifetime 200

Device # show device-tracking database
Binding Table has 8 entries, 8 dynamic (limit 200000)
```

```
Codes: L - Local, S - Static, ND - Neighbor Discovery, ARP - Address Resolution Protocol,
DH4 - IPv4 DHCP, DH6 - IPv6 DHCP, PKT - Other Packet, API - API created
Preflevel flags (prlvl):
0001:MAC and LLA match     0002:Orig trunk            0004:Orig access
0008:Orig trusted trunk    0010:Orig trusted access   0020:DHCP assigned
0040:Cga authenticated     0080:Cert authenticated    0100:Statically assigned

Network Layer Address                          Link Layer Address     Interface  vlan
prlvl      age        state      Time left
ARP 192.0.9.13                                 000a.959d.6816         Te1/0/4    200
00C8       4s         REACHABLE  699 s           <<<< new global value applied
ARP 192.0.9.12                                 000a.959d.6816         Te1/0/4    200
00C8       4s         REACHABLE  719 s           <<<< new global value applied
ARP 192.0.9.11                                 000a.959d.6816         Te1/0/4    200
00C8       4s         REACHABLE  728 s           <<<< new global value applied
ARP 192.0.9.10                                 000a.959d.6816         Te1/0/4    200
00C8       4s         REACHABLE  712 s           <<<< new global value applied
ARP 192.0.9.9                                  000a.959d.6816         Te1/0/4    200
0064       9mn        STALE      try 0 1209 s
ARP 192.0.9.8                                  000a.959d.6816         Te1/0/4    200
0064       9mn        VERIFY     5 s try 3
ARP 192.0.9.7                                  000a.959d.6816         Te1/0/4    200
0064       9mn        VERIFY     2816 ms try 3
ARP 192.0.9.6                                  000a.959d.6816         Te1/0/4    200
0064       9mn        VERIFY     1792 ms try 3
```

In this second part of the example, a policy level value is configured and the reachable lifetime is set to 50 seconds. This new reachable lifetime is again applicable only to entries created after this.

Only a reachable lifetime is configured at the policy-level and not a stale and down lifetime. This means it is still the global values that apply if the reachable lifetime of the two new entries expires and they move to the STALE or DOWN state.

```
Device(config)# device-tracking policy sisf-01
Device(config-device-tracking)# tracking enable reachable-lifetime 50
Device# show device-tracking policy sisf-01
Device-tracking policy sisf-01 configuration:
  security-level guard
  device-role node
  gleaning from Neighbor Discovery
  gleaning from DHCP6
  gleaning from ARP
  gleaning from DHCP4
  NOT gleaning from protocol unkn
  tracking enable reachable-lifetime 50    <<<< new value applies only to binding entries
created after this and on interfaces and VLANs where this policy is attached.
Policy sisf-01 is applied on the following targets:
Target               Type  Policy               Feature        Target range
Te1/0/4              PORT  sisf-01              Device-tracking vlan 200

Device# show device-tracking database
Binding Table has 10 entries, 10 dynamic (limit 200000)
Codes: L - Local, S - Static, ND - Neighbor Discovery, ARP - Address Resolution Protocol,
DH4 - IPv4 DHCP, DH6 - IPv6 DHCP, PKT - Other Packet, API - API created
Preflevel flags (prlvl):
0001:MAC and LLA match     0002:Orig trunk            0004:Orig access
0008:Orig trusted trunk    0010:Orig trusted access   0020:DHCP assigned
0040:Cga authenticated     0080:Cert authenticated    0100:Statically assigned


Network Layer Address                          Link Layer Address     Interface  vlan
prlvl      age        state      Time left
ARP 192.0.9.21                                 000a.959d.6816         Te1/0/4    200
```

```
0064       5s         REACHABLE  45 s           <<<< new policy-level value applied
ARP 192.0.9.20                                 000a.959d.6816         Te1/0/4    200
0064       5s         REACHABLE  46 s           <<<< new policy-level value applied
ARP 192.0.9.13                                 000a.959d.6816         Te1/0/4    200
00C8       14mn       STALE     try 0 865 s
ARP 192.0.9.12                                 000a.959d.6816         Te1/0/4    200
00C8       14mn       STALE     try 0 183 s
ARP 192.0.9.11                                 000a.959d.6816         Te1/0/4    200
00C8       14mn       STALE     try 0 178 s
ARP 192.0.9.10                                 000a.959d.6816         Te1/0/4    200
00C8       14mn       STALE     try 0 165 s
ARP 192.0.9.9                                  000a.959d.6816         Te1/0/4    200
0064       23mn       STALE     try 0 327 s
ARP 192.0.9.8                                  000a.959d.6816         Te1/0/4    200
0064       23mn       STALE     try 0 286 s
ARP 192.0.9.7                                  000a.959d.6816         Te1/0/4    200
0064       23mn       STALE     try 0 303 s
ARP 192.0.9.6                                  000a.959d.6816         Te1/0/4    200
0064       23mn       STALE     try 0 306 s

Device# show device-tracking database <<<< checking binding table again after new policy-level
 reachable-lifetime expires
Binding Table has 7 entries, 7 dynamic (limit 200000)
Codes: L - Local, S - Static, ND - Neighbor Discovery, ARP - Address Resolution Protocol,
DH4 - IPv4 DHCP, DH6 - IPv6 DHCP, PKT - Other Packet, API - API created
Preflevel flags (prlvl):
0001:MAC and LLA match     0002:Orig trunk            0004:Orig access
0008:Orig trusted trunk    0010:Orig trusted access   0020:DHCP assigned
0040:Cga authenticated     0080:Cert authenticated    0100:Statically assigned

Network Layer Address                          Link Layer Address     Interface  vlan
prlvl      age        state      Time left
ARP 192.0.9.21                                 000a.959d.6816         Te1/0/4    200
0064       3mn        STALE     try 0 887 s  <<<< global value applies for stale-lifetime;
  policy-level value was not configured
ARP 192.0.9.20                                 000a.959d.6816         Te1/0/4    200
0064       3mn        STALE     try 0 884 s  <<<< global value applies for stale-lifetime;
  policy-level value was not configured
ARP 192.0.9.13                                 000a.959d.6816         Te1/0/4    200
00C8       17mn       STALE     try 0 664 s
ARP 192.0.9.9                                  000a.959d.6816         Te1/0/4    200
0064       27mn       STALE     try 0 136 s
ARP 192.0.9.8                                  000a.959d.6816         Te1/0/4    200
0064       27mn       STALE     try 0 96 s
ARP 192.0.9.7                                  000a.959d.6816         Te1/0/4    200
0064       27mn       STALE     try 0 108 s
ARP 192.0.9.6                                  000a.959d.6816         Te1/0/4    200
0064       27mn       STALE     try 0 111 s
```

Example: Creating a Static Binding Entry

The following example shows you how to create a static binding entry. The "S" at the beginning of the entry indicates that it is a static binding entry

```
Device(config)# device-tracking binding vlan 100 192.0.2.1 interface tengigabitethernet1/0/1
 00:00:5e:00:53:af reachable-lifetime infinite
Device(config)# exit
Device# show device-tracking database
Binding Table has 2 entries, 0 dynamic (limit 200000)
Codes: L - Local, S - Static, ND - Neighbor Discovery, ARP - Address Resolution Protocol,
DH4 - IPv4 DHCP, DH6 - IPv6 DHCP, PKT - Other Packet, API - API created
Preflevel flags (prlvl):
0001:MAC and LLA match     0002:Orig trunk            0004:Orig access
0008:Orig trusted trunk    0010:Orig trusted access   0020:DHCP assigned
```

```
0040:Cga authenticated     0080:Cert authenticated    0100:Statically assigned


    Network Layer Address                    Link Layer Address     Interface  vlan
prlvl      age        state      Time left                    S   192.0.2.1
               0000.5e00.53af         Te1/0/1    100        0100       14s        REACHABLE
  N/A
```

Example: Global vs Policy-Level Address Limits

The following example show you how to assess which address limit is reached, when you configure address limits at the global level and at the policy-level.

The global level settings refer to the values configured for the following command string: **device-tracking bindingmax-entries** *no_of_entries* [**mac-limit** *no_of_entries* | **port-limit** *no_of_entries* | **vlan-limit** *no_of_entries*]

The policy level parameter refers to the **limit address-count** option in the device-tracking configuration mode.

For this first part of the example, the configuration is as follows:

- Global configuration: max-entries=30, vlan-limit=25, port-limit=20, mac-limit=19.
- Policy-level configuration: limit address-count=45.

The output of the **show device-tracking database details** privileged EXEC command shows that the port limit (`max/port`) is reached first. A maximum of 20 entries are allowed on a port or interface. No further binding entries are created after this. While the mac limit is configured with a lower absolute value (19), the output of the **show device-tracking database mac** privileged EXEC command shows that there are only 3 unique MAC address in the list of binding entries in the table - this limit is therefore not reached.

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# device-tracking binding max-entries 30 vlan-limit 25 port-limit 20 mac-limit
 19
Device(config)# device-tracking policy sisf-01
Device(config-device-tracking)# limit address-count 45
Device(config-device-tracking)# end
Device# show device-tracking policy sisf-01
Device-tracking policy sisf-01 configuration:
  security-level guard
  device-role node
  gleaning from Neighbor Discovery
  gleaning from DHCP6
  gleaning from ARP
  gleaning from DHCP4
  NOT gleaning from protocol unkn
  limit address-count 45
Policy sisf-01 is applied on the following targets:
Target              Type  Policy              Feature        Target range
Te1/0/4             PORT  sisf-01             Device-tracking vlan 200

Device# show device-tracking database details
 Binding table configuration:
 ---------------------------
 max/box  : 30
 max/vlan : 25
 max/port : 20
 max/mac  : 19

 Binding table current counters:
 ------------------------------
```

```
 dynamic  : 20
 local    : 0
 total    : 20    <<<< no further entries created after this.

 Binding table counters by state:
 ---------------------------------
 REACHABLE  : 20
   total    : 20
<output truncated>

Device# show device-tracking database
Binding Table has 20 entries, 20 dynamic (limit 30)
Codes: L - Local, S - Static, ND - Neighbor Discovery, ARP - Address Resolution Protocol,
DH4 - IPv4 DHCP, DH6 - IPv6 DHCP, PKT - Other Packet, API - API created
Preflevel flags (prlvl):
0001:MAC and LLA match     0002:Orig trunk            0004:Orig access
0008:Orig trusted trunk    0010:Orig trusted access   0020:DHCP assigned
0040:Cga authenticated     0080:Cert authenticated    0100:Statically assigned

Network Layer Address                          Link Layer Address     Interface  vlan
prlvl      age        state      Time left
ARP 192.0.9.39                                 000c.959d.6816         Te1/0/4    200
0064       14s        REACHABLE  37 s
ARP 192.0.9.38                                 000b.959d.6816         Te1/0/4    200
0064       14s        REACHABLE  37 s
ARP 192.0.9.37                                 000b.959d.6816         Te1/0/4    200
0064       14s        REACHABLE  36 s
ARP 192.0.9.36                                 000b.959d.6816         Te1/0/4    200
0064       14s        REACHABLE  39 s
ARP 192.0.9.35                                 000b.959d.6816         Te1/0/4    200
0064       14s        REACHABLE  38 s
ARP 192.0.9.34                                 000b.959d.6816         Te1/0/4    200
0064       14s        REACHABLE  37 s
ARP 192.0.9.33                                 000b.959d.6816         Te1/0/4    200
0064       15s        REACHABLE  36 s
ARP 192.0.9.32                                 000b.959d.6816         Te1/0/4    200
0064       15s        REACHABLE  37 s
ARP 192.0.9.31                                 000b.959d.6816         Te1/0/4    200
0064       15s        REACHABLE  36 s
ARP 192.0.9.30                                 000b.959d.6816         Te1/0/4    200
0064       15s        REACHABLE  36 s
ARP 192.0.9.29                                 000b.959d.6816         Te1/0/4    200
0064       15s        REACHABLE  35 s
ARP 192.0.9.28                                 000a.959d.6816         Te1/0/4    200
0064       15s        REACHABLE  36 s
ARP 192.0.9.27                                 000a.959d.6816         Te1/0/4    200
0064       16s        REACHABLE  35 s
ARP 192.0.9.26                                 000a.959d.6816         Te1/0/4    200
0064       16s        REACHABLE  36 s
ARP 192.0.9.25                                 000a.959d.6816         Te1/0/4    200
0064       16s        REACHABLE  34 s
ARP 192.0.9.24                                 000a.959d.6816         Te1/0/4    200
0064       16s        REACHABLE  35 s
ARP 192.0.9.23                                 000a.959d.6816         Te1/0/4    200
0064       16s        REACHABLE  34 s
ARP 192.0.9.22                                 000a.959d.6816         Te1/0/4    200
0064       16s        REACHABLE  36 s
ARP 192.0.9.21                                 000a.959d.6816         Te1/0/4    200
0064       17s        REACHABLE  33 s
ARP 192.0.9.20                                 000a.959d.6816         Te1/0/4    200
0064       17s        REACHABLE  33 s

Device# show device-tracking database mac
 MAC                    Interface  vlan       prlvl      state            Time left
```

```
Policy          Input_index
000c.959d.6816         Te1/0/4    200        NO TRUST   MAC-REACHABLE    27 s
sisf-01         12
000b.959d.6816         Te1/0/4    200        NO TRUST   MAC-REACHABLE    27 s
sisf-01         12
000a.959d.6816         Te1/0/4    200        NO TRUST   MAC-REACHABLE    27 s
sisf-01         12
```

For this second part of the example, the configuration is as follows:

- Global configuration: max-entries=30, vlan-limit=25, port-limit=20, mac-limit=19.
- Policy-level configuration: limit address-count=14.

The limit that is reached first is the policy-level, **limit address-count**. A maximum of 14 IP addresses (IPv4 and 1Pv6) are allowed on the port or interface where policy "sisf-01" is applied. No further binding entries are created after this. While the mac limit is configured with a lower absolute value (19), there are only 3 unique MAC address in the list of binding entries in the table - this limit is therefore not reached.

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# device-tracking policy sisf-01
Device(config-device-tracking)# limit address-count 14
Device(config-device-tracking)# end
Device# show device-tracking policy sisf-01
Device-tracking policy sisf-01 configuration:
  security-level guard
  device-role node
  gleaning from Neighbor Discovery
  gleaning from DHCP6
  gleaning from ARP
  gleaning from DHCP4
  NOT gleaning from protocol unkn
  limit address-count 14
Policy sisf-01 is applied on the following targets:
Target              Type  Policy              Feature        Target range
Te1/0/4             PORT  sisf-01             Device-tracking vlan 200
```

After the stale lifetime of all the existing entries has expired and the entries have been removed from the binding table, new entries are added according to the reconfigured values:

```
Device# show device-tracking database  <<<<checking time left for stale-lifetime to expire
 for existing entries.
Binding Table has 20 entries, 20 dynamic (limit 30)
Codes: L - Local, S - Static, ND - Neighbor Discovery, ARP - Address Resolution Protocol,
DH4 - IPv4 DHCP, DH6 - IPv6 DHCP, PKT - Other Packet, API - API created
Preflevel flags (prlvl):
0001:MAC and LLA match     0002:Orig trunk            0004:Orig access
0008:Orig trusted trunk    0010:Orig trusted access   0020:DHCP assigned
0040:Cga authenticated     0080:Cert authenticated    0100:Statically assigned

Network Layer Address                          Link Layer Address     Interface  vlan
prlvl      age        state     Time left
ARP 192.0.9.39                                 000c.959d.6816         Te1/0/4    200
0064       13mn       STALE     try 0 316 s
ARP 192.0.9.38                                 000b.959d.6816         Te1/0/4    200
0064       13mn       STALE     try 0 279 s
ARP 192.0.9.37                                 000b.959d.6816         Te1/0/4    200
0064       13mn       STALE     try 0 308 s
ARP 192.0.9.36                                 000b.959d.6816         Te1/0/4    200
0064       13mn       STALE     try 0 274 s
ARP 192.0.9.35                                 000b.959d.6816         Te1/0/4    200
```

```
0064       13mn       STALE     try 0 279 s
ARP 192.0.9.34                                 000b.959d.6816         Te1/0/4    200
0064       13mn       STALE     try 0 261 s
ARP 192.0.9.33                                 000b.959d.6816         Te1/0/4    200
0064       13mn       STALE     try 0 258 s
ARP 192.0.9.32                                 000b.959d.6816         Te1/0/4    200
0064       13mn       STALE     try 0 263 s
ARP 192.0.9.31                                 000b.959d.6816         Te1/0/4    200
0064       13mn       STALE     try 0 266 s
ARP 192.0.9.30                                 000b.959d.6816         Te1/0/4    200
0064       13mn       STALE     try 0 273 s
ARP 192.0.9.29                                 000b.959d.6816         Te1/0/4    200
0064       13mn       STALE     try 0 277 s
ARP 192.0.9.28                                 000a.959d.6816         Te1/0/4    200
0064       13mn       STALE     try 0 282 s
ARP 192.0.9.27                                 000a.959d.6816         Te1/0/4    200
0064       13mn       STALE     try 0 272 s
ARP 192.0.9.26                                 000a.959d.6816         Te1/0/4    200
0064       13mn       STALE     try 0 268 s
ARP 192.0.9.25                                 000a.959d.6816         Te1/0/4    200
0064       13mn       STALE     try 0 244 s
ARP 192.0.9.24                                 000a.959d.6816         Te1/0/4    200
0064       13mn       STALE     try 0 248 s
ARP 192.0.9.23                                 000a.959d.6816         Te1/0/4    200
0064       13mn       STALE     try 0 284 s
ARP 192.0.9.22                                 000a.959d.6816         Te1/0/4    200
0064       13mn       STALE     try 0 241 s
ARP 192.0.9.21                                 000a.959d.6816         Te1/0/4    200
0064       13mn       STALE     try 0 256 s
ARP 192.0.9.20                                 000a.959d.6816         Te1/0/4    200
0064       13mn       STALE     try 0 243 s

Device# show device-tracking database  <<<no output indicates no entries in the database


Device# show device-tracking database details

 Binding table configuration:
 ----------------------------
 max/box  : 30
 max/vlan : 25
 max/port : 20
 max/mac  : 19

 Binding table current counters:
 -------------------------------
 dynamic  : 14
 local    : 0
 total    : 14

 Binding table counters by state:
 --------------------------------
 REACHABLE  : 14
   total    : 14
<output truncated>

Device# show device-tracking database
Binding Table has 14 entries, 14 dynamic (limit 30)
Codes: L - Local, S - Static, ND - Neighbor Discovery, ARP - Address Resolution Protocol,
DH4 - IPv4 DHCP, DH6 - IPv6 DHCP, PKT - Other Packet, API - API created
Preflevel flags (prlvl):
0001:MAC and LLA match     0002:Orig trunk            0004:Orig access
0008:Orig trusted trunk    0010:Orig trusted access   0020:DHCP assigned
0040:Cga authenticated     0080:Cert authenticated    0100:Statically assigned
```

```
Network Layer Address                          Link Layer Address     Interface  vlan
prlvl      age        state      Time left
ARP 192.0.9.68                                 0001.5e00.53af         Te1/0/4    200
0064       4s         REACHABLE  48 s
ARP 192.0.9.67                                 0001.5e00.53af         Te1/0/4    200
0064       4s         REACHABLE  48 s
ARP 192.0.9.66                                 0001.5e00.53af         Te1/0/4    200
0064       4s         REACHABLE  47 s
ARP 192.0.9.65                                 0001.5e00.53af         Te1/0/4    200
0064       4s         REACHABLE  48 s
ARP 192.0.9.64                                 0001.5e00.53af         Te1/0/4    200
0064       4s         REACHABLE  46 s
ARP 192.0.9.63                                 0000.5e00.53af         Te1/0/4    200
0064       7s         REACHABLE  44 s
ARP 192.0.9.62                                 0000.5e00.53af         Te1/0/4    200
0064       7s         REACHABLE  45 s
ARP 192.0.9.61                                 0000.5e00.53af         Te1/0/4    200
0064       7s         REACHABLE  43 s
ARP 192.0.9.60                                 0000.5e00.53af         Te1/0/4    200
0064       7s         REACHABLE  44 s
ARP 192.0.9.59                                 0000.5e00.53af         Te1/0/4    200
0064       7s         REACHABLE  44 s
ARP 192.0.9.58                                 0000.5e00.53af         Te1/0/4    200
0064       8s         REACHABLE  44 s
ARP 192.0.9.57                                 0000.5e00.53af         Te1/0/4    200
0064       8s         REACHABLE  44 s
ARP 192.0.9.56                                 0000.5e00.53af         Te1/0/4    200
0064       10s        REACHABLE  41 s
ARP 192.0.9.55                                 0000.5e00.53af         Te1/0/4    200
0064       10s        REACHABLE  40 s

Device# show device-tracking database mac
 MAC                    Interface  vlan       prlvl      state            Time left
 Policy           Input_index
 0001.5e00.53af         Te1/0/4    200        NO TRUST   MAC-REACHABLE    30 s
 sisf-01          12
 0000.5e00.53af         Te1/0/4    200        NO TRUST   MAC-REACHABLE    30 s
 sisf-01          12
```

Example: Setting VLAN, Port, and MAC Limits to Default Values

The following example shows you how to reset one or more limits to their default values.

```
Device(config)# device-tracking binding max-entries 30 vlan-limit 25 port-limit 20 mac-limit
 19 <<<< all three limits configured.
Device(config)#exit
Device# show device-tracking database details

 Binding table configuration:
 ----------------------------
 max/box  : 30
 max/vlan : 25
 max/port : 20
 max/mac  : 19
<output truncated>

Device# configure terminal
Device(config)# device-tracking binding max-entries 30 vlan-limit 25 <<<< only VLAN limit
configured;  port-limit and mac-limit keywords leftout.
Device(config)# exit
Device# show device-tracking database details

 Binding table configuration:
 ----------------------------
```

```
 max/box  : 30
 max/vlan : 25
 max/port : no limit    <<<reset to default
 max/mac  : no limit    <<<reset to default
```

Example: Global vs Policy-Level Limits Relating to MAC Addresses

The following example shows how precendence is determined for global and policy-level MAC limits. The global value specifies the maximum number of entries allowed per MAC address. The policy-level IPv4 per MAC and IPv6 per MAC limits, which may be present only in a programmatic policy, specify the number of IPv4 and IPv6 addresses allowed per MAC address.

In the first part of the example, the global value (10 entries allowed per MAC address) is higher than the policy-level setting (3 IPv4 addresses allowed for each MAC address). The `Binding table current counters`, in the output of the **show device-tracking database details** privileged EXEC command shows that and the limit that is reached first is the policy level limit.

Note No configuration is displayed for the policy-level setting, because you cannot *configure* the "IPv4 per mac" or the "IPv6 per mac" in any policy. In this example, the DT-PROGRAMMATIC policy is applied to target by configuring the **ip dhcp snooping vlan** *vlan* command in global configuration mode. The IPv4 per mac limit exists, because the programmatically created policy has a limit for this parameter.

```
Device# configure terminal
Device(config)# ip dhcp snooping vlan 200
Device(config)# end
Device# show device-tracking policy DT-PROGRAMMATIC
Policy DT-PROGRAMMATIC configuration:
  security-level glean (*)
  device-role node
  gleaning from Neighbor Discovery
  gleaning from DHCP
  gleaning from ARP
  gleaning from DHCP4
  NOT gleaning from protocol unkn
  limit address-count for IPv4 per mac 3 (*)
  tracking enable
Policy DT-PROGRAMMATIC is applied on the following targets:
Target      Type    Policy               Feature            Target range
Te1/0/4     PORT    DT-PROGRAMMATIC      Device-tracking    vlan 200

  note:
  Binding entry Down timer: 24 hours (*)
  Binding entry Stale timer:   24 hours (*)

Device(config)# device-tracking binding max-entries 50 mac-limit 10
Device# show device-tracking database details
Binding table configuration:
 ----------------------------
 max/box  : 50
 max/vlan : no limit
 max/port : no limit
 max/mac  : 10

 Binding table current counters:
 -------------------------------
 dynamic  : 3
 local    : 0
 total    : 3
```

```
 Binding table counters by state:
 --------------------------------
 REACHABLE  : 2
   total    : 3

Device# show device-tracking database
Binding Table has 3 entries, 3 dynamic (limit 50)
Codes: L - Local, S - Static, ND - Neighbor Discovery, ARP - Address Resolution Protocol,
DH4 - IPv4 DHCP, DH6 - IPv6 DHCP, PKT - Other Packet, API - API created
Preflevel flags (prlvl):
0001:MAC and LLA match     0002:Orig trunk            0004:Orig access
0008:Orig trusted trunk    0010:Orig trusted access   0020:DHCP assigned
0040:Cga authenticated     0080:Cert authenticated    0100:Statically assigned


Network Layer Address                   Link Layer Address     Interface  vlan       prlvl
      age       state      Time left
ARP 192.0.9.8                            000a.959d.6816         Te1/0/4    200        0064
       4s        REACHABLE  25 s
ARP 192.0.9.7                            000a.959d.6816         Te1/0/4    200        0064
       4s        REACHABLE  27 s
ARP 192.0.9.6                            000a.959d.6816         Te1/0/4    200        0064
       55s       VERIFY     5s try 2
<<<<<<policy-level limit reached;  only up to 3 IPv4 addresses per MAC address are allowed.


Device# show device-tracking database mac
 MAC                   Interface  vlan       prlvl      state            Time left
 Policy           Input_index
 000a.959d.6816        Te1/0/4    200        NO TRUST   MAC-STALE        93585 s
 DT-PROGRAMMATIC          12
```

In the second part of the example, the global value (2 entries allowed per MAC address) is lower than the policy-level setting (3 IPv4 addresses allowed for each MAC address). The `Binding table current counters`, in the output of the **show device-tracking database details** privileged EXEC command shows that and the limit that is reached first is the policy level limit.

```
Device# show device-tracking policy DT-PROGRAMMATIC

Policy DT-PROGRAMMATIC configuration:
  security-level glean (*)
  device-role node
  gleaning from Neighbor Discovery
  gleaning from DHCP
  gleaning from ARP
  gleaning from DHCP4
  NOT gleaning from protocol unkn
  limit address-count for IPv4 per mac 3 (*)
  tracking enable
Policy DT-PROGRAMMATIC is applied on the following targets:
Target      Type    Policy               Feature            Target range
Te1/0/4     PORT    DT-PROGRAMMATIC      Device-tracking    vlan 200

  note:
  Binding entry Down timer: 24 hours (*)
  Binding entry Stale timer:   24 hours (*)

Device(config)# device-tracking binding max-entries 50 mac-limit 2
Device# show device-tracking database details
Binding table configuration:
 ---------------------------
```

```
 max/box  : 50
 max/vlan : no limit
 max/port : no limit
 max/mac  : 2

 Binding table current counters:
 -------------------------------
 dynamic  : 2
 local    : 0
 total    : 2

 Binding table counters by state:
 ---------------------------------
 REACHABLE  : 2
   total    : 2

Device# show device-tracking database
Binding Table has 3 entries, 3 dynamic (limit 50)
Codes: L - Local, S - Static, ND - Neighbor Discovery, ARP - Address Resolution Protocol,
DH4 - IPv4 DHCP, DH6 - IPv6 DHCP, PKT - Other Packet, API - API created
Preflevel flags (prlvl):
0001:MAC and LLA match     0002:Orig trunk            0004:Orig access
0008:Orig trusted trunk    0010:Orig trusted access   0020:DHCP assigned
0040:Cga authenticated     0080:Cert authenticated    0100:Statically assigned


Network Layer Address                   Link Layer Address     Interface  vlan       prlvl
      age       state      Time left
ARP 192.0.9.3                            000a.959d.6816         Te1/0/4    200        0064
       5s        REACHABLE   27 s
ARP 192.0.9.4                            000a.959d.6816         Te1/0/4    200        0064
       6s        REACHABLE   20 s

<<<<<<global limit reached;  only up to 2 binding entries per MAC address is allowed.

Device# show device-tracking database mac
 MAC                   Interface  vlan       prlvl      state            Time left
 Policy           Input_index
 000a.959d.6816         Te1/0/4    200        NO TRUST   MAC-STALE        93585 s
 DT-PROGRAMMATIC       12
```

device-tracking logging

To log snooping security events like packet drops, unresolved packets, and suspected MAC or IP theft, configure the **device-tracking logging** command in global configuration mode. To disable logging, enter the **no** form of the command.

device-tracking logging [**packet drop** | **resolution-veto** | **theft**]

no device-tracking logging [**packet drop** | **resolution-veto** | **theft**]

Syntax Description

packet drop	Logs packet drop events.
resolution-veto	Logs unresolved packet events.
theft	Logs IP and MAC theft events.

Command Default

Events are not logged.

Command Modes

Global configuration [Device(config)#]

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Logs generated for snooping security events have a severity level of 4 (meaning, warnings). For example:

```
%SISF-4-PAK_DROP: Message dropped A=FE80::20D:FF:FE0E:F G=- V=10 I=Tu0 P=NDP::RA Reason=Packet not authorized on port
```

You can view snooping security logs by entering the **show logging | include SISF-4** command in privileged EXEC mode.

For information about the snooping events for which logs are generated, see the system message guide for the corresponding release: System Message Guides. Search for `SISF-4`.

Packet Drop Events

When you configure the **packet drop** keyword, a log is generated everytime a packet is dropped. The log also includes the reason for the packet drop. The reasons include and are not limited to the following:

- `Packet not authorized on port`: This means that a security feature dropped the packet because a packet of this kind is not expected on the port, based on the configuration. Examples of such security features and the situations in which a packet is dropped, include and are not limited to the following: The Router Advertisement Guard feature may decide to drop IPv6 Router Advertisement packets if they are received on ports that are not configured as router-facing ports. The DHCP Guard feature may drop packets from DHCP server (DHCP OFFER or DHCP REPLY) if they are received on a port which is not configured as server-facing port.
- `Packet accepted but not forwarded`: This means that the packet is not forwarded, but it is still considered valid to glean binding information from. This is usually seen when packets from a host are seen by SISF during the validation phase (while the binding is in a transitional state).

- `Malformed Packet dropped in Guard mode`: This means that the incoming packet is malformed and cannot be parsed properly.
- `Packet is throttled`: This means the packet was dropped because it exceeds the throttling limit for packets within a time interval. The system allows a maximum of 50 packets in 5 seconds.
- `Silent drop`: This happens to packets that are generated either by device-tracking instances to communicate among the different instances across multiple switches, or as a response to an action trigged by device-tracking. For instance, a response on the probe that was initiated by the device-tracking, to determine the reachability status of the host reachability.
- `Martian packet`: This means that the incoming packet was dropped because it has Martian source IP address, such as, a multicast, loopback, or unspecified address.
- `Martian mac`: This means that the incoming packet was dropped because it has a Martian MAC or Link-Layer source address.
- `Address limit per box reached`: This means that the incoming packet was dropped, because the limit configured with the **device-tracking binding max-entries** *no_of_entries* global configuration command, was reached. Enter the **show device-tracking database details** privileged EXEC command to display current limits.
- `Address limit per vlan reached`: This means that the incoming packet was dropped, because the limit configured with the **device-tracking binding max-entries** *no_of_entries* **vlan-limit** *no_of_entries* global configuration command, was reached. Enter the **show device-tracking database details** privileged EXEC command to display current limits.
- `Address limit per port reached`: This means that the incoming packet was dropped, because the limit configured with the **device-tracking binding max-entries** *no_of_entries* **port-limit** *no_of_entries* global configuration command, was reached. Enter the **show device-tracking database details** privileged EXEC command to display current limits.
- `Address limit per policy reached` : This means that the incoming packet was dropped, because the limit configured with the **limit address-count** *ip-per-port* keyword in the device-tracking configuration mode was reached. This is configured at a policy level. Enter the **show device-tracking policy***policy-name* privileged EXEC command to display current limits.
- `Address limit per mac reached`: This means that the incoming packet was dropped, because the limit configured with the **device-tracking binding max-entries** *no_of_entries* **mac-limit** *no_of_entries* global configuration command, was reached. Enter the **show device-tracking database details** privileged EXEC command to display current limits.
- `Address Family limit per mac reached`: This means that the incoming packet was dropped, because the IPv4 per MAC or IPv6 per MAC limit specified in a programmatic policy was reached. You cannot configure this policy parameter; a programmatically created policy may have either an IPv4 per MAC limit, or an IPv6 per MAC limit, or both, or neither. Enter the **show device-tracking policy***policy-name* privileged EXEC command to display the limit if it exists.

Resolution Veto Events

When you configure the **resolution-veto** keyword, a log is generated for every unresolved packet. This logging option meant to be used only if the IPv6 Destination Guard feature is also enabled.

The IPv6 Destination Guard feature ensures that the device performs address resolution only for those addresses that are known to be active on the link. All destinations that are active on the link are entered in the binding

table. When a destination is not found in the binding table, address resolution is prevented. By configuring **resolution-veto** logging you can keep track of such unresolved packets.

If the **resolution-veto** keyword is configured and the the IPv6 Destination Guard feature is not, logs are not generated.

Theft Events

When you configure the **theft** keyword, a log is generated when SISF detects an IP theft, or a MAC theft or both.

In the log, verified binding information (IP, MAC address, interface or VLAN) is preceded by the term "Known" . A suspicious IP address and MAC address is preceded by the term "New" or "Cand". Interface and VLAN information is also provided along with the suspiscious IP or MAC address - this helps you identify where the suspiscious traffic was seen.

For example, see the following MAC theft log:

```
%SISF-4-MAC_THEFT: MAC Theft Cand IP=2001::12B VLAN=70 MAC=9cfc.e85e.139d Cand I/F=Gi1/0/4
 Known IP=71.0.0.96 Known I/F=Ac0
```

These snippets of the log show the IP address of the suspiscious host and the interface on which it was seen: `Cand IP=2001::12B`, `VLAN=70`, `Cand I/F=Gi1/0/4`.

This snippet of the log shows the *known* MAC address, which the suspiscious host is using: `MAC=9cfc.e85e.139d`.

These snippets of the log show the IP address and interface of the existing, verified entry: `Known IP=71.0.0.96` and `Known I/F=Ac0`.

Examples

- Example: Packet Drop Logs, on page 1259
- Example: Theft Logs, on page 1259

Example: Packet Drop Logs

The following are examples of logs generated for packet drop events:

```
%SISF-4-PAK_DROP: Message dropped A=FE80::20D:FF:FE0E:F G=- V=10 I=Tu0 P=NDP::RA Reason=Packet
 not authorized on port

%SISF-4-PAK_DROP: Message dropped A=20.0.0.1 M=dead.beef.0001 V=20 I=Gi1/0/23 P=ARP
Reason=Packet accepted but not forwarded
```

Example: Theft Logs

The following are examples of logs generated for IP and MAC theft events:

```
%SISF-4-MAC_AND_IP_THEFT: MAC_AND_IP Theft A=FE80::EE1D:8BFF:FE9B:102 V=102 I=Vl102
M=ec1d.8b9b.0102 New=Tu0

%SISF-4-MAC_THEFT: MAC Theft IP=192.2.1.2 VLAN=102 MAC=cafe.cafe.cafe I/F=Gi1/0/3 New I/F
over fabric

%SISF-4-IP_THEFT: IP Theft IP=FE80::9873:1D5E:E6E9:1F7E VLAN=20 MAC=2079.18d5.13ad IF=Ac0
New I/F over fabric
```

```
%SISF-4-IP_THEFT: IP Theft IP=10.0.187.5 VLAN=10 Cand-MAC=0069.0000.0001 Cand-I/F=Gi1/0/23
 Known MAC over-fabric Known I/F over-fabric

%SISF-4-MAC_THEFT: MAC Theft Cand IP=2001::12B VLAN=70 MAC=9cfc.e85e.139d Cand I/F=Gi1/0/4
 Known IP=71.0.0.96 Known I/F=Ac0
```

device-tracking policy

To create a custom device-tracking policy, and to enter the device-tracking configuration mode to configure the various parameter of the policy, enter the **device-tracking policy** 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	Creates a device-tracking policy with the specified name - if it doesn't already exist. You can also specify the name of a programmatically created policy. After you configure a policy name, the device enters the device-tracking configuration mode, where you can configure policy parameters. Enter a question mark (?) at the system prompt to see the list of policy parameters that can be configured.

Command Default

SISF-based device tracking is disabled.

Command Modes

Global configuration [Device(config)#]

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

When you enter the **device-tracking policy***policy-name* command in global configuration mode, the system creates a custom policy with the specified name (if it does not already exist) and enters the device-tracking configuration mode. In this mode, you can configure policy parameters.

After you create a policy and configure its parameters, you must attach it to an interface or VLAN. Only then does the activity of extracting binding information (IP and MAC address) from packets that enter the network and the creation of binding entries, actually begin. For more information about attaching a policy, see device-tracking (interface config), on page 1231device-tracking (VLAN config), on page 1234.

To display detailed information about all the policies available on the device and the targets they are attached to, enter the **show device-tracking policies detail** command in privileged EXEC mode.

Configuring Policy Parameters

You can configure the parameters of a policy only if it is a custom policy. You cannot change the parameters of a programmatic policy. You also cannot change the parameters of the `default` policy.

To display the list of parameters for a policy, enter a question mark (?) at the system prompt in device-tracking configuration mode:

```
Device(config)# device-tracking policy sisf-01
Device(config-device-tracking)# ?
device-tracking policy configuration mode:
  data-glean            binding recovery by data traffic source address
                        gleaning
  default               Set a command to its defaults
  destination-glean     binding recovery by data traffic destination address
                        gleaning
  device-role           Sets the role of the device attached to the port
```

```
distribution-switch   Distribution switch to sync with
exit                  Exit from device-tracking policy configuration mode
limit                 Specifies a limit
medium-type-wireless  Force medium type to wireless
no                    Negate a command or set its defaults
prefix-glean          Glean prefixes in RA and DHCP-PD traffic
protocol              Sets the protocol to glean (default all)
security-level        setup security level
tracking              Override default tracking behavior
trusted-port          setup trusted port
vpc                   setup vpc port
```

Keyword	Description
data-glean	Enables learning of addresses from a data packet snooped from a source inside the network and populates the binding table with the data traffic source address. Enter one of these options: • **log-only**: Generates a syslog message upon data packet notification. • **recovery**: Uses a protocol to enable binding table recovery. Enter **NDP** or **DHCP**.
default	Sets the policy paramter to its default value. You can set these policy attributes to their default values: • **data-glean**: Source address is not learnt or gleaned. • **destination-glean**: Destination address is not learnt or gleaned • **device-role**: Node. • **distribution-switch**: Not supported. • **limit**: An address count limit is not set. • **medium-type-wireless**: <tbd> • **prefix-glean**: Prefixes are not learnt. • **protocol**: Addresses of all protocols (ARP, DHCP4, DHCP6, NDP, and UDP) are gleaned. • **security-level**: Guard. • **tracking**: Polling is disabled. • **trusted-port**: Disabled, that is, the guard function is enabled on the configured target) • **vpc**: Not supported.
destination-glean	Enables population of the binding table by gleaning the destination address of data traffic. Enter one of these options: • **log-only**: Generates a syslog message upon data packet notification. • **recovery**: Uses a protocol to enable binding table recovery. Enter **NDP** or **DHCP**.

Keyword	Description
device-role	Indicates the type of device that is facing the port and this can be one of the following: • **node**: Allows creation of binding entries for a port. • **switch**: Stops the creation of binding entries for a port. This option is suited to multi-switch set-ups, where the possibility of large device tracking tables is very high. Here, a port facing a device (an uplink trunk port) can be configured to stop creating binding entries, and the traffic arriving at such a port can be trusted, because the switch on the other side of the trunk port will have device tracking enabled and that will have checked the validity of the binding entry. This option is commonly used along with the **trusted-port** keyword. Configuring both the **device-role** and **trusted-port** options on an uplink trunk port helps build an efficient and scalable "secure zone". Both parameters must be configured to achieve an efficient distribution of the creation of binding table entries (thus keeping the binding tables smaller).
distribution-switch	Although visible on the CLI, this keyword is not supported. Any configuration does not take effect.
exit	Exits the device-tracking configuration mode and returns to global configuration mode.
limit address-count	Configures the maximum number of number of IPv4 and IPv6 addresses to be allowed per port. The purpose of this limit is to ensure that binding entries are restricted to only known and expected hosts. *ip-per-port*: Enter the maximum number of IP addresses you want to allow on a port. This limit applies to IPv4 and IPv6 addresses as a whole. When the limit is reached, no further IP addresses can be added to the binding table, and traffic from new hosts are dropped. Enter a value between 1 and 32000.
medium-type-wireless	Although visible on the CLI, this keyword is not supported. Any configuration does not take effect.

Keyword	Description
no	Negates the command, that is, reverts a policy parameter to its default value. For information about what the default value is, see the **default** keyword. • **data-glean** • **destination-glean** • **device-role** • **distribution-switch**: Not supported. • **limit address-count** • **medium-type-wireless** • **prefix-glean** • **protocol** • **security-level** • **tracking** • **trusted-port** • **vpc**: Not supported.
prefix-glean only	Enables learning of prefixes from either IPv6 Router Advertisements or from DHCP-PD. You have the following option: (Optional) **only**: Gleans only prefixes and not host addresses.
protocol	Gleans addresses of specified protocols. By default, all are gleaned. Enter one of these options: • **arp** [**prefix-list** *name*]: Gleans addresses in ARP packets. Optionally, enter the name of prefix-list that is to be matched. • **dhcp4** [**prefix-list** *name*]: Gleans addresses in DHCPv4 packets. Optionally, enter the name of prefix-list that is to be matched. • **dhcp6** [**prefix-list** *name*]: Gleans addresses in DHCPv6 packets. Optionally, enter the name of prefix-list that is to be matched. • **ndp** [**prefix-list** *name*]: Gleans addresses in NDP packets. Optionally, enter the name of prefix-list that is to be matched. • **udp** [**prefix-list** *name*]: Although visible on the CLI, this option is not supported. Any configuration does not take effect.

Keyword	Description
security-level	Specifies the level of security that is enforced. When a packet enters the network, SISF extracts the IP and MAC address (the source of the packet) and subsequent action, is dictated by the security level configured in the policy. Enter one of these options: • **glean**: Extracts the IP and MAC address and enters them into the binding table, without any verification. Use this option if you want to only *learn* about the host and not rely on SISF for authentication of the binding entry. • **guard**: Extracts the IP and MAC address and checks this information against the binding table. The outcome of the verification determines if a binding entry is added, or updated, or if the packet is dropped and the client is rejected This is the default value for the security-level parameter. • **inspect**: Although this keyword is available on the CLI, we recommend not using it. The **glean** and **guard** options described above address most use cases and network requirements.

Keyword	Description
tracking	Determines if an entry is polled after the reachable lifetime expires. Polling is a periodic and conditional checking of the host to see the state it is in, whether it is still connected, and whether it is communicating. For more information about polling, see the *Usage Guidelines* below. By default, polling is not enabled. Enter one of these options: • **disable** : Turns off polling action. [**stale-lifetime** {*seconds* | **infinite**}]: Optionally you can also configure a stale-lifetime. If you do, configure one of the following for the stale-lifetime timer: • *seconds*: Configure a value for the stale-lifetime timer. Enter a value between 1 and 86400 seconds. The default value is 86400 seconds (24 hours). • **infinite**: Disables the timer for the STALE state. This means that a timer is not started when an entry enters the STALE state and the entry remains in the STALE state, indefinitely. • **enable**: Turns on polling action. [**reachable-lifetime** [*seconds* | **infinite**]]: Optionally you can also configure a reachable-lifetime. If you do, configure one of the following for the reachable-lifetime timer: • *seconds*: Configure a value for the reachable-lifetime timer. Enter a value between 1 and 86400 seconds. The default value is 300 seconds (5 minutes). • **infinite**: Disables the timer for the REACHABLE state. This means that a timer is not started when an entry enters the REACHABLE state and the entry remains in the REACHABLE state, indefinitely.
trusted-port	This option disables the guard function on configured targets. Bindings learned through a trusted-port have preference over bindings learned through any other port. A trusted port is also given preference in case of a collision while making an entry in the table. This option is commonly used along with the **device-role** keyword. Configuring both the **device-role** and **trusted-port** options on an uplink trunk port helps achieve an efficient distribution of the creation of binding table entries (thus keeping the binding tables smaller).
vpc	Although visible on the CLI, this option is not supported. Any configuration does not take effect.

Global versus Poicy-Level Settings

You configure policy parameters in the device-tracking configuration mode and what you configure for a policy applies only to that policy. Some of the policy parameters have counterparts in the global configuration mode. For detailed information about the parameters that have global-level counterparts and to know which value takes precendence (whether the globally configured or the policy-level value), see: device-tracking binding, on page 1237.

Polling a Host

If you configure the **tracking** policy parameter, the switch sends a polling request after the reachable lifetime expires. The switch polls the host up to 3 times at fixed, system-determined intervals. You can also specify an interval by using the **device-tracking tracking retry-interval** *seconds* command in global configuration mode. The polling request is in the form of an Address Resolution Protocol (ARP) probe or a Neighbor Solicitation message. During this time the state of the entry changes to VERIFY.

If a polling response is received (thus confirming reachability of the host), the state of the entry changes back to REACHABLE. If the switch does not receive a polling response after 3 attempts, the entry changes to the STALE state.

Note Using the **tracking** policy parameter, you can enable or disable polling at a policy-level regardless of whether the polling is enabled or disabled at the global configuration level (the **device-tracking tracking** command in global configuration mode. See Example: Disabling Polling at a Policy-Level, on page 1268and device-tracking tracking, on page 1274.

Changing the Limit Address-Count

If you configure a limit using the **limit address-count** policy parameter and then change it - the new limit is applicable only to entries learned after the change. Further, regardless of whether the new limit is higher or lower than the previous limit, existing entries are not affected and are allowed to go through their binding entry lifecycle.

If the binding table is full (in accordance with the previous limit), any new entries are not added until the existing entries complete their lifecycle. SISF attempts to create space for new entries by identifying and removing only *inactive* entries . But if the entries are active, they are not removed and are allowed to go through their binding entry lifecycle.

If you want to make the new lower limit take effect immediately, you can use either one of these options:

- Enter the **clear device-tracking database** command in privileged EXEC mode and specify an interface or VLAN. This removes all existing entries from the database of only the specified target. New entries are then learned and added as per the current limit address-count settings. See Example: Changing the Address Count Limit, on page 1268.
- Remove and reattach the policy on the required target. Enter the **no device-tracking policy***policy-name* command in interface or VLAN configuration mode to remove the policy. Removing the policy from an interface or VLAN removes the bindings that are attached to the target. Enter the **device-tracking policy***policy-name* command in interface or VLAN configuration mode to reattach it. Reattaching the policy causes learning of all the binding entries according to the new limit.

Examples

- Example: Disabling Polling at a Policy-Level, on page 1268
- Example: Changing the Address Count Limit, on page 1268

Example: Disabling Polling at a Policy-Level

The following example shows how you can disable polling at the policy-level even if polling is enabled at the global level. Here, polling is disabled for all interfaces and VLANs were policy `sisf-01` is applied.

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# device-tracking tracking
Device(config)# exit
Device# show running-config | include device-tracking device-tracking tracking
device-tracking policy sisf-01
 device-tracking attach-policy sisf-01
 device-tracking attach-policy sisf-01 vlan 200
device-tracking binding reachable-lifetime 700 stale-lifetime 1000 down-lifetime 200
device-tracking binding logging

Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# device-tracking policy sisf-01
Device(config-device-tracking)# tracking disable
Device(config-device-tracking)# end
Device# show device-tracking policy sisf-01
Device-tracking policy sisf-01 configuration:
  security-level guard
  device-role node
  gleaning from Neighbor Discovery
  gleaning from DHCP6
  gleaning from ARP
  gleaning from DHCP4
  NOT gleaning from protocol unkn
  limit address-count 5
  tracking disable
Policy sisf-01 is applied on the following targets:
Target               Type  Policy               Feature        Target range
Te1/0/4              PORT  sisf-01              Device-tracking vlan 200
vlan 200             VLAN  sisf-01              Device-tracking vlan all
```

Example: Changing the Address Count Limit

The following example shows you how to make a change in the **limit address-count** policy parameter setting take effect immediately. In this example, the clear command is used to remove all entries from the binding table for the changed settings to take effect immediately.

```
Device# show device-tracking policy sisf-01
Device-tracking policy sisf-01 configuration:
  security-level guard
  device-role node
  gleaning from Neighbor Discovery
  gleaning from DHCP6
  gleaning from ARP
  gleaning from DHCP4
  NOT gleaning from protocol unkn
  limit address-count 25
Policy sisf-01 is applied on the following targets:
Target               Type  Policy               Feature        Target range
Te1/0/4              PORT  sisf-01              Device-tracking vlan 200
vlan 200             VLAN  sisf-01              Device-tracking vlan all

Device# show running-config | include device-tracking
```

```
device-tracking policy sisf-01
 device-tracking attach-policy sisf-01
 device-tracking attach-policy sisf-01 vlan 200
device-tracking binding reachable-lifetime 700 stale-lifetime 1000 down-lifetime 200
device-tracking binding logging


*Dec 13 15:08:50.723: %SISF-6-ENTRY_CREATED: Entry created IP=192.0.9.25 VLAN=200
MAC=001b.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:08:50.723: %SISF-6-ENTRY_CREATED: Entry created IP=192.0.9.26 VLAN=200
MAC=001b.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:08:50.724: %SISF-6-ENTRY_CREATED: Entry created IP=192.0.9.27 VLAN=200
MAC=001b.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:08:50.724: %SISF-6-ENTRY_CREATED: Entry created IP=192.0.9.28 VLAN=200
MAC=001b.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:08:50.724: %SISF-6-ENTRY_CREATED: Entry created IP=192.0.9.29 VLAN=200
MAC=001b.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:08:50.724: %SISF-6-ENTRY_CREATED: Entry created IP=192.0.9.30 VLAN=200
MAC=001b.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:08:50.725: %SISF-6-ENTRY_CREATED: Entry created IP=192.0.9.31 VLAN=200
MAC=001b.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:08:50.725: %SISF-6-ENTRY_CREATED: Entry created IP=192.0.9.32 VLAN=200
MAC=001b.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:08:50.725: %SISF-6-ENTRY_CREATED: Entry created IP=192.0.9.33 VLAN=200
MAC=001b.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:08:50.725: %SISF-6-ENTRY_CREATED: Entry created IP=192.0.9.34 VLAN=200
MAC=001c.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:08:50.726: %SISF-6-ENTRY_CREATED: Entry created IP=192.0.9.35 VLAN=200
MAC=001c.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:08:50.726: %SISF-6-ENTRY_CREATED: Entry created IP=192.0.9.36 VLAN=200
MAC=001c.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:08:50.726: %SISF-6-ENTRY_CREATED: Entry created IP=192.0.9.37 VLAN=200
MAC=001c.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:08:50.726: %SISF-6-ENTRY_CREATED: Entry created IP=192.0.9.38 VLAN=200
MAC=001c.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:08:50.727: %SISF-6-ENTRY_CREATED: Entry created IP=192.0.9.39 VLAN=200
MAC=001c.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:08:50.727: %SISF-6-ENTRY_CREATED: Entry created IP=192.0.9.40 VLAN=200
MAC=001c.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:08:50.727: %SISF-6-ENTRY_CREATED: Entry created IP=192.0.9.41 VLAN=200
MAC=001c.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:08:50.727: %SISF-6-ENTRY_CREATED: Entry created IP=192.0.9.42 VLAN=200
MAC=001c.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:08:50.728: %SISF-6-ENTRY_CREATED: Entry created IP=192.0.9.43 VLAN=200
MAC=001c.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:08:50.728: %SISF-6-ENTRY_MAX_ORANGE: Reaching 80% of max adr allowed per policy
 (25) V=200 I=Te1/0/4 M=001d.4411.3ab7
*Dec 13 15:08:50.728: %SISF-6-ENTRY_CREATED: Entry created IP=192.0.9.44 VLAN=200
MAC=001d.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:08:50.728: %SISF-6-ENTRY_CREATED: Entry created IP=192.0.9.45 VLAN=200
MAC=001d.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:08:50.728: %SISF-6-ENTRY_CREATED: Entry created IP=192.0.9.46 VLAN=200
MAC=001d.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:08:50.729: %SISF-6-ENTRY_CREATED: Entry created IP=192.0.9.47 VLAN=200
MAC=001d.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:08:50.729: %SISF-6-ENTRY_CREATED: Entry created IP=192.0.9.48 VLAN=200
MAC=001d.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:08:50.729: %SISF-6-ENTRY_CREATED: Entry created IP=192.0.9.49 VLAN=200
MAC=001d.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF

Device# show device-tracking database Binding Table has 25 entries, 25 dynamic (limit 200000)
Codes: L - Local, S - Static, ND - Neighbor Discovery, ARP - Address Resolution Protocol,
DH4 - IPv4 DHCP, DH6 - IPv6 DHCP, PKT - Other Packet, API - API created
Preflevel flags (prlvl):
```

```
0001:MAC and LLA match     0002:Orig trunk           0004:Orig access
0008:Orig trusted trunk    0010:Orig trusted access  0020:DHCP assigned
0040:Cga authenticated     0080:Cert authenticated   0100:Statically assigned


    Network Layer Address                  Link Layer Address     Interface  vlan
prlvl      age        state      Time left
ARP 192.0.9.49                             001d.4411.3ab7         Te1/0/4    200
00FF       22s        REACHABLE  699 s
ARP 192.0.9.48                             001d.4411.3ab7         Te1/0/4    200
00FF       22s        REACHABLE  691 s
ARP 192.0.9.47                             001d.4411.3ab7         Te1/0/4    200
00FF       22s        REACHABLE  687 s
ARP 192.0.9.46                             001d.4411.3ab7         Te1/0/4    200
00FF       22s        REACHABLE  714 s
ARP 192.0.9.45                             001d.4411.3ab7         Te1/0/4    200
00FF       22s        REACHABLE  692 s
ARP 192.0.9.44                             001d.4411.3ab7         Te1/0/4    200
00FF       22s        REACHABLE  702 s
ARP 192.0.9.43                             001c.4411.3ab7         Te1/0/4    200
00FF       22s        REACHABLE  680 s
ARP 192.0.9.42                             001c.4411.3ab7         Te1/0/4    200
00FF       22s        REACHABLE  708 s
ARP 192.0.9.41                             001c.4411.3ab7         Te1/0/4    200
00FF       22s        REACHABLE  683 s
ARP 192.0.9.40                             001c.4411.3ab7         Te1/0/4    200
00FF       22s        REACHABLE  708 s
ARP 192.0.9.39                             001c.4411.3ab7         Te1/0/4    200
00FF       22s        REACHABLE  710 s
ARP 192.0.9.38                             001c.4411.3ab7         Te1/0/4    200
00FF       22s        REACHABLE  697 s
ARP 192.0.9.37                             001c.4411.3ab7         Te1/0/4    200
00FF       22s        REACHABLE  707 s
ARP 192.0.9.36                             001c.4411.3ab7         Te1/0/4    200
00FF       22s        REACHABLE  695 s
ARP 192.0.9.35                             001c.4411.3ab7         Te1/0/4    200
00FF       22s        REACHABLE  708 s
ARP 192.0.9.34                             001c.4411.3ab7         Te1/0/4    200
00FF       22s        REACHABLE  706 s
ARP 192.0.9.33                             001b.4411.3ab7         Te1/0/4    200
00FF       22s        REACHABLE  683 s
ARP 192.0.9.32                             001b.4411.3ab7         Te1/0/4    200
00FF       22s        REACHABLE  697 s
ARP 192.0.9.31                             001b.4411.3ab7         Te1/0/4    200
00FF       22s        REACHABLE  683 s
ARP 192.0.9.30                             001b.4411.3ab7         Te1/0/4    200
00FF       22s        REACHABLE  678 s
ARP 192.0.9.29                             001b.4411.3ab7         Te1/0/4    200
00FF       22s        REACHABLE  696 s
ARP 192.0.9.28                             001b.4411.3ab7         Te1/0/4    200
00FF       22s        REACHABLE  704 s
ARP 192.0.9.27                             001b.4411.3ab7         Te1/0/4    200
00FF       22s        REACHABLE  713 s
ARP 192.0.9.26                             001b.4411.3ab7         Te1/0/4    200
00FF       22s        REACHABLE  695 s
ARP 192.0.9.25                             001b.4411.3ab7         Te1/0/4    200
00FF       22s        REACHABLE  686 s
```

The address count limit is changed from 25 to a lower limit of 5. But because the existing entries have not completed their binding entry lifecycle, they are not deleted from the binding table. In order to make the new address count limit of 5 take effect immediately, the **clear device-tracking database** command is used to delete all existing entries. New entries are then learned and added as per the current limit address-count settings.

```
Device# configure terminal
Device(config)# device-tracking policy sisf-01
Device(config-device-tracking)# limit address-count 5
Device(config-device-tracking)# end
Device# show device-tracking policy sisf-01
Device-tracking policy sisf-01 configuration:
  security-level guard
  device-role node
  gleaning from Neighbor Discovery
  gleaning from DHCP6
  gleaning from ARP
  gleaning from DHCP4
  NOT gleaning from protocol unkn
  limit address-count 5
Policy sisf-01 is applied on the following targets:
Target              Type  Policy              Feature        Target range
Te1/0/4             PORT  sisf-01             Device-tracking vlan 200
vlan 200            VLAN  sisf-01             Device-tracking vlan all

Device# show device-tracking database
Binding Table has 25 entries, 25 dynamic (limit 200000)
Codes: L - Local, S - Static, ND - Neighbor Discovery, ARP - Address Resolution Protocol,
DH4 - IPv4 DHCP, DH6 - IPv6 DHCP, PKT - Other Packet, API - API created
Preflevel flags (prlvl):
0001:MAC and LLA match     0002:Orig trunk            0004:Orig access
0008:Orig trusted trunk    0010:Orig trusted access   0020:DHCP assigned
0040:Cga authenticated     0080:Cert authenticated    0100:Statically assigned


    Network Layer Address                    Link Layer Address     Interface  vlan
prlvl      age        state      Time left
ARP 192.0.9.49                               001d.4411.3ab7         Te1/0/4    200
00FF       67s        REACHABLE  654 s
ARP 192.0.9.48                               001d.4411.3ab7         Te1/0/4    200
00FF       67s        REACHABLE  646 s
ARP 192.0.9.47                               001d.4411.3ab7         Te1/0/4    200
00FF       67s        REACHABLE  642 s
ARP 192.0.9.46                               001d.4411.3ab7         Te1/0/4    200
00FF       67s        REACHABLE  669 s
ARP 192.0.9.45                               001d.4411.3ab7         Te1/0/4    200
00FF       67s        REACHABLE  647 s
ARP 192.0.9.44                               001d.4411.3ab7         Te1/0/4    200
00FF       67s        REACHABLE  657 s
ARP 192.0.9.43                               001c.4411.3ab7         Te1/0/4    200
00FF       67s        REACHABLE  635 s
ARP 192.0.9.42                               001c.4411.3ab7         Te1/0/4    200
00FF       67s        REACHABLE  663 s
ARP 192.0.9.41                               001c.4411.3ab7         Te1/0/4    200
00FF       67s        REACHABLE  638 s
ARP 192.0.9.40                               001c.4411.3ab7         Te1/0/4    200
00FF       67s        REACHABLE  663 s
ARP 192.0.9.39                               001c.4411.3ab7         Te1/0/4    200
00FF       67s        REACHABLE  665 s
ARP 192.0.9.38                               001c.4411.3ab7         Te1/0/4    200
00FF       67s        REACHABLE  652 s
ARP 192.0.9.37                               001c.4411.3ab7         Te1/0/4    200
00FF       67s        REACHABLE  662 s
ARP 192.0.9.36                               001c.4411.3ab7         Te1/0/4    200
00FF       67s        REACHABLE  650 s
ARP 192.0.9.35                               001c.4411.3ab7         Te1/0/4    200
00FF       67s        REACHABLE  663 s
ARP 192.0.9.34                               001c.4411.3ab7         Te1/0/4    200
00FF       67s        REACHABLE  661 s
```

```
ARP 192.0.9.33                              001b.4411.3ab7         Te1/0/4    200
00FF       67s        REACHABLE  637 s
ARP 192.0.9.32                              001b.4411.3ab7         Te1/0/4    200
00FF       67s        REACHABLE  652 s
ARP 192.0.9.31                              001b.4411.3ab7         Te1/0/4    200
00FF       67s        REACHABLE  638 s
ARP 192.0.9.30                              001b.4411.3ab7         Te1/0/4    200
00FF       67s        REACHABLE  633 s
ARP 192.0.9.29                              001b.4411.3ab7         Te1/0/4    200
00FF       67s        REACHABLE  651 s
ARP 192.0.9.28                              001b.4411.3ab7         Te1/0/4    200
00FF       67s        REACHABLE  658 s
ARP 192.0.9.27                              001b.4411.3ab7         Te1/0/4    200
00FF       67s        REACHABLE  668 s
ARP 192.0.9.26                              001b.4411.3ab7         Te1/0/4    200
00FF       67s        REACHABLE  650 s
ARP 192.0.9.25                              001b.4411.3ab7         Te1/0/4    200
00FF       67s        REACHABLE  641 s

Device# clear device-tracking database

*Dec 13 15:10:22.837: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.49 VLAN=200
MAC=001d.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:10:22.838: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.48 VLAN=200
MAC=001d.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:10:22.838: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.47 VLAN=200
MAC=001d.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:10:22.838: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.46 VLAN=200
MAC=001d.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:10:22.839: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.45 VLAN=200
MAC=001d.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:10:22.839: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.44 VLAN=200
MAC=001d.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:10:22.839: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.43 VLAN=200
MAC=001c.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:10:22.839: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.42 VLAN=200
MAC=001c.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:10:22.840: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.41 VLAN=200
MAC=001c.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:10:22.840: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.40 VLAN=200
MAC=001c.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:10:22.840: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.39 VLAN=200
MAC=001c.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:10:22.841: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.38 VLAN=200
MAC=001c.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:10:22.841: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.37 VLAN=200
MAC=001c.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:10:22.841: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.36 VLAN=200
MAC=001c.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:10:22.842: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.35 VLAN=200
MAC=001c.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:10:22.842: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.34 VLAN=200
MAC=001c.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:10:22.842: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.33 VLAN=200
MAC=001b.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:10:22.842: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.32 VLAN=200
MAC=001b.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:10:22.843: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.31 VLAN=200
MAC=001b.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:10:22.843: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.30 VLAN=200
MAC=001b.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:10:22.843: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.29 VLAN=200
MAC=001b.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:10:22.844: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.28 VLAN=200
```

```
MAC=001b.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:10:22.844: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.27 VLAN=200
MAC=001b.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:10:22.844: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.26 VLAN=200
MAC=001b.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:10:22.844: %SISF-6-ENTRY_DELETED: Entry deleted IP=192.0.9.25 VLAN=200
MAC=001b.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF

Device# show device-tracking database
<no output; binding table cleared>

*Dec 13 15:11:38.346: %SISF-6-ENTRY_CREATED: Entry created IP=192.0.9.25 VLAN=200
MAC=001b.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:11:38.346: %SISF-6-ENTRY_CREATED: Entry created IP=192.0.9.26 VLAN=200
MAC=001b.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:11:38.347: %SISF-6-ENTRY_CREATED: Entry created IP=192.0.9.27 VLAN=200
MAC=001b.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:11:38.347: %SISF-6-ENTRY_MAX_ORANGE: Reaching 80% of max adr allowed per policy
 (5) V=200 I=Te1/0/4 M=001b.4411.3ab7
*Dec 13 15:11:38.347: %SISF-6-ENTRY_CREATED: Entry created IP=192.0.9.28 VLAN=200
MAC=001b.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF
*Dec 13 15:11:38.347: %SISF-6-ENTRY_CREATED: Entry created IP=192.0.9.29 VLAN=200
MAC=001b.4411.3ab7 I/F=Te1/0/4 Preflevel=00FF

Device# show device-tracking database
Binding Table has 5 entries, 5 dynamic (limit 200000)
Codes: L - Local, S - Static, ND - Neighbor Discovery, ARP - Address Resolution Protocol,
DH4 - IPv4 DHCP, DH6 - IPv6 DHCP, PKT - Other Packet, API - API created
Preflevel flags (prlvl):
0001:MAC and LLA match     0002:Orig trunk            0004:Orig access
0008:Orig trusted trunk    0010:Orig trusted access   0020:DHCP assigned
0040:Cga authenticated     0080:Cert authenticated    0100:Statically assigned


    Network Layer Address                    Link Layer Address     Interface  vlan
prlvl      age        state      Time left
ARP 192.0.9.29                               001b.4411.3ab7         Te1/0/4    200
00FF       15s        REACHABLE  716 s
ARP 192.0.9.28                               001b.4411.3ab7         Te1/0/4    200
00FF       15s        REACHABLE  702 s
ARP 192.0.9.27                               001b.4411.3ab7         Te1/0/4    200
00FF       15s        REACHABLE  705 s
ARP 192.0.9.26                               001b.4411.3ab7         Te1/0/4    200
00FF       15s        REACHABLE  716 s
ARP 192.0.9.25                               001b.4411.3ab7         Te1/0/4    200
00FF       15s        REACHABLE  718 s
```

device-tracking tracking

To enable polling for IPv4 and IPv6 and configure the polling parameters, configure the **device-tracking tracking** command in global configuration mode. To disable polling, enter the **no** form of the command.

Note This command does not enable the SISF-based device-tracking feature. It enables configuration of polling parameters on a device where the device-tracking feature is enabled.

device-tracking tracking [**auto-source** [**fallback** *ipv4_and_fallback_source_mask ip_prefix_mask* [**override**] | **retry-interval** *seconds*]

no device-tracking tracking [**auto-source** | **retry-interval**]

Syntax Description

auto-source	Causes the source address of an Address Resolution Protocol (ARP) probe to be sourced in the following order of preference: • The first preference is to set the source address to the VLAN SVI, if an SVI is configured. • The second preference is to locate an IP-MAC binding entry in device-tracking table, from same subnet and use that as the source address. • The third and last preference is to use 0.0.0.0 as the source address.
fallback *ipv4_and_fallback_source_maskip_prefix_mask*	Causes the source address of an ARP probe to be sourced in the following order of preference: • The first preference is to set the source address to the VLAN SVI, if an SVI is configured. • The second preference is to locate an IP-MAC binding entry in device-tracking table, from same subnet and use that as the source address. • The third and last preference is to compute the source address from the client's IPv4 address and the mask provided. The source MAC address is taken from the MAC address of the switchport facing the client. If you configure the **fallback** keyword, you must also specify an IP address and mask.

override	Causes the source address of an ARP probe to be sourced in the following order of preference: • The first preference is to set the source address to the VLAN SVI, if this is configured. • The second and last preference is to use 0.0.0.0 as the source address. **Note** This keyword configures SISF to *not* select the source address from the binding table. We do not recommend using this option if an SVI is not configured.
retry-interval *seconds*	Configures a multiplicative factor or "base value", for the backoff algorithm. The backoff algorithm determines the wait time between the 3 polling attempts that occur after reachable lifetime expiry. Enter a value between 1 and 3600 seconds. The default value is one. When polling, there is an increasing wait time between the 3 polling attempts or retries. The backoff algorithm determines this wait time. The value you configure for the retry interval is multiplied by the backoff algorithm's wait time. For example, if the backoff algorithm determines a wait time of 2, 4, and 6 seconds between the 3 attempts respectively, and you configure a retry interval of 2 seconds, the actual interval you will observe is as follows: 2*2 seconds of wait time before the first polling attempt, 2*4 seconds for the second polling attempt and 2*6 for the third polling attempt. If polling is enabled, but a retry interval is not configured, the switch polls the host up to 3 times at system-determined intervals. This configuration applies to ARP probes and Neighbor Solicitation messages.

Command Default

Polling is disabled by default.

Command Modes

Global configuration [Device(config)#]

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Polling is a periodic and conditional checking of the host to see the state it is in, whether it is still connected, and whether it is communicating. Polling enables you to assess the continued presence of a tracked device.

Polling occurs at these junctures: 3 times after the reachable lifetime timer expires, and a final attempt at stale lifetime expiry.

- In an IPv4 network, polling is in the form of an ARP probe. Here, the switch sends unicast ARP probes to the connected host, to determine the host's reachability status. When sending ARP probes, the system constructs packets according to RFC 5227 specifications.
- In an IPv6 network, polling is in the form of a Neighbor Solicitation message. Here, the switch verifies reachability of a connected host by using the unicast address of the connected host as the destination address.

Configure the **device-tracking tracking** command in global configuration mode, to enable polling for IPv4 and IPv6.

Also configure the **retry-interval** *seconds* to configure the polling interval after reachable lifetime timer expiry.

Note The **auto-source**, **fallback** *ipv4_and_fallback_source_maskip_prefix_mask* , and **override** keywords apply only to ARP probes and not Neighbor Solicitation messages.

The value you configure for **retry-interval** *seconds* keywords applies to both IPv4 and IPv6.

Enter the **show running-config | include device-tracking** display current polling settings. For example:

```
Device# show running-config | include device-tracking
device-tracking tracking retry-interval 2
device-tracking policy sisf-01
 device-tracking attach-policy sisf-01 vlan 200
device-tracking binding reachable-lifetime 50 stale-lifetime 150 down-lifetime 30
device-tracking binding logging
```

Enter the **show device-tracking database** command in privileged EXEC mode, to display the duration of the various lifetimes of an entry. While polling, the system changes the state of the entry to VERIFY. Check the `Time left` column in the output to observe the duration.

When you track the reachable and stale lifetime of an entry with the **show device-tracking database** command, and polling is enabled, you may notice that the STALE lifetime is sometimes shorter than what you have configured. This is because the time required for polling is *subtracted* from the stale lifetime.

Global versus Policy-Level Settings for Polling

After you configure **device-tracking tracking** command in global configuration mode, you still have the flexibility to turn polling on or off, for individual interfaces and VLANs. For this you must enable or disable polling in the policy. Note how the global and policy-level settings interact:

Global Setting	Policy-Level Setting	Result
Polling is enabled at the global level. `Device(config)# device-tracking tracking`	Polling is enabled on an interface or VLAN. `Device(config-device-tracking)# tracking enable`	Polling is effective on the interface or VLAN.
	Polling is disabled on an interface or VLAN. `Device(config-device-tracking)# tracking disable`	Polling is not effective on the interface or VLAN.
	Default polling is configured on the interface or VLAN. `Device(config-device-tracking)# default tracking`	Because polling is enabled at the *global* config level, polling is effective on the interface or VLAN.
	The **no** form of the command is configured on the interface or VLAN. `Device(config-device-tracking)# no tracking`	The **no** form of the command sets the command to its default. But because polling is enabled at the *global* config level, polling is effective on the interface or VLAN.
Polling is disabled at the global level. `Device(config)# no device-tracking tracking`	Polling is enabled on an interface or VLAN. `Device(config-device-tracking)# tracking enable`	Polling is effective on the interface or VLAN.
	Polling is disabled on an interface or VLAN. `Device(config-device-tracking)# tracking disable`	Polling is not effective on the interface or VLAN.
	Default polling is configured on the interface or VLAN. `Device(config-device-tracking)# default tracking`	Polling is not effective on the interface or VLAN.
	The **no** form of the command is configured on the interface or VLAN. `Device(config-device-tracking)# no tracking`	Polling is not effective on the interface or VLAN.

device-tracking upgrade-cli

To convert legacy IP Device Tracking (IPDT) and IPv6 Snooping commands to SISF commands, configure the **device-tracking upgrade-cli** command in global configuration mode. To revert to legacy commands, enter the **no** form of the command.

device-tracking upgrade-cli [**force** | **revert**]

no device-tracking upgrade-cli [**force** | **revert**]

Syntax Description

force	Skips the confirmation step and converts legacy IPDT and IPv6 Snooping commands to SISF commands.
revert	Reverts to legacy IPDT and IPv6 Snooping commands.

Command Default

Legacy IPDT and IPv6 Snooping commands remain as-is.

Command Modes

Global configuration [Device(config)#]

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Based on the legacy configuration that exists on your device, the **device-tracking upgrade-cli** command upgrades your CLI differently. Consider the following configuration scenarios and the corresponding migration results before you migrate your existing configuration.

Note You cannot configure a mix of the old IPDT and IPv6 snooping CLI with the SISF-based device tracking CLI.

Only IPDT Configuration Exists

If your device has only IPDT configuration, running the **device-tracking upgrade-cli** command converts the configuration to use the new SISF policy that is created and attached to the interface. You can then update this SISF policy.

If you continue to use the legacy commands, this restricts you to operate in a legacy mode where only the legacy IPDT and IPv6 snooping commands are available on the device.

Only IPv6 Snooping Configuration Exists

On a device with existing IPv6 snooping configuration, the old IPv6 Snooping commands are available for further configuration. The following options are available:

- (Recommended) Use the **device-tracking upgrade-cli** command to convert all your legacy configuration to the new SISF-based device tracking commands. After conversion, only the new device tracking commands will work on your device.

- Use the legacy IPv6 Snooping commands for your future configuration and do not run the **device-tracking upgrade-cli** command. With this option, only the legacy IPv6 Snooping commands are available on your device, and you cannot use the new SISF-based device tracking CLI commands.

Both IPDT and IPv6 Snooping Configuration Exist

On a device that has both legacy IPDT configuration and IPv6 snooping configuration, you can convert legacy commands to the SISF-based device tracking CLI commands. However, note that only one snooping policy can be attached to an interface, and the IPv6 snooping policy parameters override the IPDT settings.

Note If you do not migrate to the new SISF-based commands and continue to use the legacy IPv6 snooping or IPDT commands, your IPv4 device tracking configuration information may be displayed in the IPv6 snooping commands, as the SISF-based device tracking feature handles both IPv4 and IPv6 configuration. To avoid this, we recommend that you convert your legacy configuration to SISF-based device tracking commands.

No IPDT or IPv6 Snooping Configuration Exists

If your device has no legacy IP Device Tracking or IPv6 Snooping configurations, you can use only the new SISF-based device tracking commands for all your future configuration. The legacy IPDT commands and IPv6 snooping commands are not available.

Examples

The following example shows you how to convert IPv6 Snooping commands to SISF-based device-tracking commands.

```
Device# show ipv6 snooping features
Feature name   priority state
Device-tracking   128   READY
Source guard       32   READY

Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# device-tracking upgrade-cli
 IPv6 Snooping and IPv4 device tracking CLI will be
 converted to the new top level device-tracking CLI
Are you sure ? [yes]: yes
Number of Snooping Policies Upgraded: 2
Device(config)# exit
```

After conversion, only the new SISF-based device-tracking commands will work on your device:

```
Device# show ipv6 snooping features
                          ^
% Invalid input detected at '^' marker.

Device# show device-tracking features
Feature name   priority state
Device-tracking   128   READY
Source guard       32   READY

Device# show device-tracking policies
Target               Type  Policy               Feature        Target range
```

```
Te1/0/4             PORT  sisf-01             Device-tracking vlan 200
vlan 200            VLAN  sisf-01             Device-tracking vlan all
```

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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

Command	Description
authentication logging verbose	Filters details from authentication syst
dot1x logging verbose	Filters details from 802.1x system mes
mab logging verbose	Filters details from MAC authenticatio

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	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

dot1x supplicant controlled transient
no dot1x supplicant controlled transient

Syntax Description

This command has no arguments or keywords.

Command Default

Access is allowed to 802.1x supplicant ports during authentication.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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# configure terminal
Device(config)# dot1x supplicant force-multicast
Device(config)# end
```

Related Commands

Command	Description
cisp enable	Enables CISP on a device so that it
dot1x credentials	Configures the 802.1x supplicant c
dot1x pae supplicant	Configures an interface to act only

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Use this command to test the IEEE 802.1x capability of the devices connected to all ports or to specific ports on a switch.

There is not a no form of this command.

This example shows how to enable the IEEE 802.1x readiness check on a switch to query a port. It also shows the response received from the queried port verifying that the device connected to it is IEEE 802.1x-capable:

```
Device> 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

Command	Description
dot1x test timeout *timeout*	Configures the timeout used to w readiness query.

dot1x test timeout

To configure the timeout used to wait for EAPOL response from a port being queried for IEEE 802.1x readiness, use the **dot1x test timeout** command in global configuration mode.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Use this command to configure the timeout used to wait for EAPOL response.

There is not a no form of this command.

This example shows how to configure the switch to wait 27 seconds for an EAPOL response:

```
Device> enable
Device# dot1x test timeout 27
```

You can verify the timeout configuration status by entering the **show running-config** command.

Related Commands

Command	Description
dot1x test eapol-capable [**interface** *interface-id*]	Checks for IEEE 802.1x readiness on devices connected to all or to specified IEEE 802.1x-capable ports.

dot1x timeout

To configure the value for retry timeouts, use the **dot1x timeout** command in global configuration or interface configuration mode. To return to the default value for retry timeouts, use the **no** form of this command.

dot1x timeout { **auth-period** *seconds* | **held-period** *seconds* | **quiet-period** *seconds* | **ratelimit-period** *seconds* | **server-timeout** *seconds* | **start-period** *seconds* | **supp-timeout** *seconds* | **tx-period** *seconds* }

Syntax Description

auth-period *seconds*	Configures the time, in seconds for which a supplicant will stay in the HELD state (that is, the length of time it will wait before trying to send the credentials again after a failed attempt). The range is from 1 to 65535. The default is 30.
held-period *seconds*	Configures the time, in seconds for which a supplicant will stay in the HELD state (that is, the length of time it will wait before trying to send the credentials again after a failed attempt). The range is from 1 to 65535. The default is 60
quiet-period *seconds*	Configures the time, in seconds, that the authenticator (server) remains quiet (in the HELD state) following a failed authentication exchange before trying to reauthenticate the client. The range is from 1 to 65535. The default is 60
ratelimit-period *seconds*	Throttles the EAP-START packets that are sent from misbehaving client PCs (for example, PCs that send EAP-START packets that result in the wasting of 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 *seconds*	Configures the interval, in seconds, between two successive EAPOL-Start frames when they are being retransmitted. • The range is from 1 to 65535. The default is 30. If the server does not send a response to an 802.1X packet within the specified period, the packet is sent again.
start-period *seconds*	Configures the interval, in seconds, between two successive EAPOL-Start frames when they are being retransmitted. The range is from 1 to 65535. The default is 30.

supp-timeout *seconds*	Sets the authenticator-to-supplicant retransmission time for all EAP messages other than EAP Request ID. The range is from 1 to 65535. The default is 30.
tx-period *seconds*	Configures the number of seconds between retransmission of EAP request ID packets (assuming that no response is received) to the client. • The range is from 1 to 65535. The default is 30. • If an 802.1X packet is sent to the supplicant and the supplicant does not send a response after the retry period, the packet will be sent again.

Command Default

Periodic reauthentication and periodic rate-limiting are done.

Command Modes

Global configuration (config)

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

You should change the default value of this command only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain clients and authentication servers.

The **dot1x timeout reauth-period** interface configuration command affects the behavior of the 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
```

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

Release	Modification
	This command was introduced.

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

Command	Description
show aaa servers	Displays information related to the DTLS server.
clear aaa counters servers radius {*server id* | **all**}	Clears the RADIUS DTLS-specific statistics.
debug radius dtls	Enables RADIUS DTLS-specific debugs.

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

level *level*	(Optional) Specifies the level for which the password is applicable. You can specif levels, using numbers 0 through 15. Level 1 is normal user EXEC mode user privil specified in the command or in the **no** form of the command, the privilege level de
0	(Optional) Specifies an unencrypted cleartext password. The password is converte Algorithm (SHA) 256 secret and is stored in the device.
unencrypted-password	Specifies the password to enter enable mode.
encryption-type	(Optional) Cisco-proprietary algorithm used to encrypt the password. If you specify next argument that you supply must be an encrypted password (a password already device). You can specify type 7, which indicates that a hidden password follows.
encrypted-password	Encrypted password copied from another device configuration.

Command Default

No password is defined.

Command Modes

Global configuration (config)

Command History

Release	Modificat
Cisco IOS XE Fuji 16.9.2	This comm

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.

Caution 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.

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 Crtl-V when you create the password, for example, to create the password *abc?123,* do the following:
  1. Enter **abc**.
  2. Press **Crtl-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 enables the password pswd2 for privilege level 2:

```
Device> enable
Device# configure terminal
Device(config)# enable password level 2 pswd2
```

The following example shows how to set the encrypted password 1i5Rkls3LoyxzS8t9, which has been copied from a device configuration file, for privilege level 2 using encryption type 7:

```
Device> enable
Device# configure terminal
Device(config)# enable password level 2 5 $1$i5Rkls3LoyxzS8t9
```

Related Commands

Command	Description
enable secret	Specifies an additional layer of security over the **enable**
service password-encryption	Encrypts a password.
more nvram:startup-config	Displays the startup configuration file contained in NVR CONFIG_FILE environment variable.
privilege level	Sets the privilege level for the user.

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

level *level*	(Optional) Specifies the level for which the password is applicable. You can specify levels, using numerals 1 through 15. Level 1 is normal user EXEC mode privileges. If in the command or in the **no** form of the command, the privilege level defaults to 15
0	(Optional) Specifies an unencrypted cleartext password. The password is converted Algorithm (SHA) 256 secret and is stored in the device.
unencrypted-password	Specifies the password for users to enter enable mode. This password should be differer created with the **enable password** command.
encryption-type	Cisco-proprietary algorithm used to hash the password: • **5**: Specifies a message digest algorithm 5-encrypted (MD5-encrypted) secret. • **8**: Specifies a Password-Based Key Derivation Function 2 (PBKDF2) with SHA • **9**: Specifies a scrypt-hashed secret.
encrypted-password	Hashed password that is copied from another device configuration.

Command Default

No password is defined.

Command Modes

Global configuration (config)

Command History

Release	Modificat
Cisco IOS XE Fuji 16.9.2	This comm

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 Crtl-v when you create the password; for example, to create the password *abc?123,* do the following:
  1. Enter **abc**.
  2. Press **Crtl-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 1FaD0$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

Command	Description
enable password	Sets a local password to control access to various privilege
more nvram:startup-config	Displays the startup configuration file contained in NVRAM CONFIG_FILE environment variable.
service password-encryption	Encrypt passwords.

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 Fuji 16.9.2	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)# exit
```

Related Commands

Command	Description
show running-config	Displays the contents of the current running configuration file.

include-icv-indicator

To include the integrity check value (ICV) indicator in MKPDU, use the **include-icv-indicator** command in MKA-policy configuration mode. To disable the ICV indicator, use the **no** form of this command.

include-icv-indicator
no include-icv-indicator

Syntax Description

This command has no arguments or keywords.

Command Default

ICV indicator is included.

Command Modes

MKA-policy configuration (config-mka-policy)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Examples

The following example shows how to include the ICV indicator in MKPDU:

```
Device> enable
Device# configure terminal
Device(config)# mka policy 2
Device(config-mka-policy)# include-icv-indicator
```

Related Commands

Command	Description
mka policy	Configures an MKA policy.
confidentiality-offset	Sets the confidentiality offset for MACsec operations.
delay-protection	Configures MKA to use delay protection in sending MKPDU.
key-server	Configures MKA key-server options.
macsec-cipher-suite	Configures cipher suite for deriving SAK.
sak-rekey	Configures the SAK rekey interval.
send-secure-announcements	Configures MKA to send secure announcements in sending MKPDUs.
ssci-based-on-sci	Computes SSCI based on the SCI.
use-updated-eth-header	Uses the updated Ethernet header for ICV calculation.

ip access-list

To define an IP access list or object-group access control list (ACL) by name or number or to enable filtering for packets with IP helper-address destinations, use the **ip access-list** command in global configuration mode. To remove the IP access list or object-group ACL or to disable filtering for packets with IP helper-address destinations, use the **no** form of this command.

ip access-list {{**extended** | **resequence** | **standard**}{*access-list-numberaccess-list-name*} | **helper egress check** | **log-update threshold** *threshold-number* | **logging** {**hash-generation** | **interval** *time*} | **persistent** | **role-based** *access-list-name*}
ip access-list {{**extended** | **resequence** | **standard**}{*access-list-numberaccess-list-name*} | **helper egress check** | **log-update threshold** | **logging** {**hash-generation** | **interval**} | **persistent** | **role-based** *access-list-name*}

Syntax Description

standard	Specifies a standard IP access list.
resequence	Specifies a resequenced IP access list.
extended	Specifies an extended IP access list. Required for object-group ACLs.
access-list-name	Name of the IP access list or object-group ACL. Names cannot contain a space or quotation mark, and must begin with an alphabetic character to prevent ambiguity with numbered access lists.
access-list-number	Number of the access list. • A standard IP access list is in the ranges 1-99 or 1300-1999. • An extended IP access list is in the ranges 100-199 or 2000-2699.
helper egress check	Enables permit or deny matching capability for an outbound access list that is applied to an interface, for traffic that is relayed via the IP helper feature to a destination server address.
log-update	Controls the access list log updates.
threshold *threshold-number*	Sets the access list logging threshold. The range is 0 to 2147483647.
logging	Controls the access list logging.
hash-generation	Enables syslog hash code generation.
interval *time*	Sets the access list logging interval in milliseconds. The range is 0 to 2147483647.
persistent	Access control entry (ACE) sequence numbers are persistent across reloads. **Note** This is enabled by default and cannot be disabled.
role-based	Specifies a role-based IP access list.

Command Default

No IP access list or object-group ACL is defined, and outbound ACLs do not match and filter IP helper relayed traffic.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Use this command to configure a named or numbered IP access list or an object-group ACL. This command places the device in access-list configuration mode, where you must define the denied or permitted access conditions by using the **deny** and **permit** commands.

Specifying the **standard** or **extended** keyword with the **ip access-list** command determines the prompt that appears when you enter access-list configuration mode. You must use the **extended** keyword when defining object-group ACLs.

You can create object groups and IP access lists or object-group ACLs independently, which means that you can use object-group names that do not yet exist.

Use the **ip access-group** command to apply the access list to an interface.

The **ip access-list helper egress check** command enables outbound ACL matching for permit or deny capability on packets with IP helper-address destinations. When you use an outbound extended ACL with this command, you can permit or deny IP helper relayed traffic based on source or destination User Datagram Protocol (UDP) ports. The **ip access-list helper egress check** command is disabled by default; outbound ACLs will not match and filter IP helper relayed traffic.

Examples

The following example defines a standard access list named Internetfilter:

```
Device> enable
Device# configure terminal
Device(config)# ip access-list standard Internetfilter
Device(config-std-nacl)# permit 192.168.255.0 0.0.0.255
Device(config-std-nacl)# permit 10.88.0.0 0.0.255.255
Device(config-std-nacl)# permit 10.0.0.0 0.255.255.255
```

The following example shows how to create an object-group ACL that permits packets from the users in my_network_object_group if the protocol ports match the ports specified in my_service_object_group:

```
Device> enable
Device# configure terminal
Device(config)# ip access-list extended my_ogacl_policy
Device(config-ext-nacl)# permit tcp object-group my_network_object_group portgroup
 my_service_object_group any
Device(config-ext-nacl)# deny tcp any any
```

The following example shows how to enable outbound ACL filtering on packets with helper-address destinations:

```
Device> enable
Device# configure terminal
Device(config)# ip access-list helper egress check
```

Related Commands

Command	Description
deny	Sets conditions in a named IP access list or in an object-group ACL that will deny packets.
ip access-group	Applies an ACL or an object-group ACL to an interface or a service policy map.
object-group network	Defines network object groups for use in object-group ACLs.
object-group service	Defines service object groups for use in object-group ACLs.
permit	Sets conditions in a named IP access list or in an object-group ACL that will permit packets.
show ip access-list	Displays the contents of IP access lists or object-group ACLs.
show object-group	Displays information about object groups that are configured.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

For SGACL logging, you must configure the **permit ip log** command. Also, this command must be configured in Cisco Identity Services Engine (ISE) to enable logging for dynamic SGACLs.

The following example shows how to define an SGACL that can be applied to IPv4 traffic and enter role-based access list configuration mode:

```
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

Command	Description
permit ip log	Permits logging that matches the configured entry.
show ip access-list	Displays contents of all current IP access lists.

ip admission

To enable web authentication, use the **ip admission** command in interface configuration mode 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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The **ip admission** command applies a web authentication rule to a switch port.

This example shows how to apply a web authentication rule to a switchport:

```
Device> 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

name	Name of network admission control rule.
consent	Associates an authentication proxy consent web page with the IP admission rule specified using the *admission-name* argument.
proxy http	Configures web authentication custom page.
absolute-timer *minutes*	(Optional) Elapsed time, in minutes, before the external server times out.
inactivity-time *minutes*	(Optional) Elapsed time, in minutes, before the external file server is deemed unreachable.
list	(Optional) Associates the named rule with an access control list (ACL).
acl	Applies a standard, extended list to a named admission control rule. The value ranges from 1 through 199, or from 1300 through 2699 for expanded range.
acl-name	Applies a named access list to a named admission control rule.
service-policy type tag	(Optional) A control plane service policy is to be configured.
service-policy-name	Control plane tag service policy that is configured using the **policy-map type control tag***policyname* command, keyword, and argument. This policy map is used to apply the actions on the host when a tag is received.

Command Default

Web authentication is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The **ip admission name** command globally enables web authentication on a switch.

After you enable web authentication on a switch, use the **ip access-group in** and **ip admission web-rule** interface configuration commands to enable web authentication on a specific interface.

Examples

This example shows how to configure only web authentication on a switch port:

```
Device> 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

Command	Description
dot1x fallback	Configures a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication.
fallback profile	Creates a web authentication fallback profile.
ip admission	Enables web authentication on a port.
show authentication sessions interface *interface* **detail**	Displays information about the web authentication session status.
show ip admission	Displays information about NAC cached entries or the NAC configuration.

ip dhcp snooping database

To configure the Dynamic Host Configuration Protocol (DHCP)-snooping database, use the **ip dhcp snooping database** command in global configuration mode. To disable the DHCP-snooping database, use the **no** form of this command.

ip dhcp snooping database { **crashinfo:** *url* | **flash:** *url* | **ftp:** *url* | **http:** *url* | **https:** *url* | **rcp:** *url* | **scp:** *url* | **tftp:** *url* | **timeout** *seconds* | **usbflash0:** *url* | **write-delay** *seconds* }
no ip dhcp snooping database [**timeout** | **write-delay**]
abor

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 cancel timeout interval; valid values are from 0 to 86400 seconds.
usbflash0:*url*	Specifies the database URL for storing entries using USB flash.

write-delay *seconds*	Specifies the amount of time before writing the DHCP-snooping entries to an external server after a change is seen in the local DHCP-snooping database; valid values are from 15 to 86400 seconds.

Command Default

The DHCP-snooping database is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

You must enable DHCP snooping on the interface before entering this command. Use the **ip dhcp snooping** command to enable DHCP snooping.

This example shows how to specify the database URL using TFTP:

```
Device> 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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

You must globally enable DHCP snooping by using the **ip dhcp snooping** global configuration command for any DHCP snooping configuration to take effect.

When the option-82 feature is enabled, the default remote-ID suboption is the 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
```

ip dhcp snooping verify no-relay-agent-address

To disable the DHCP snooping feature from verifying that the relay agent address (giaddr) in a DHCP client message matches the client hardware address on an untrusted port, use the **ip dhcp snooping verify no-relay-agent-address** command in global configuration mode. To enable verification, use the **no** form of this command.

ip dhcp snooping verify no-relay-agent-address
no ip dhcp snooping verify no-relay-agent-address

Syntax Description

This command has no arguments or keywords.

Command Default

The DHCP snooping feature verifies that the relay-agent IP address (giaddr) field in DHCP client message on an untrusted port is 0.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

By default, the DHCP snooping feature verifies that the relay-agent IP address (giaddr) field in DHCP client message on an untrusted port is 0; the message is dropped if the giaddr field is not 0. Use the **ip dhcp snooping verify no-relay-agent-address** command to disable the verification. Use the **no ip dhcp snooping verify no-relay-agent-address** to reenable verification.

This example shows how to enable verification of the giaddr in a DHCP client message:

```
Device> 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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

If this command is configured, the specified access list is assigned to the HTTP server. Before the HTTP server accepts a connection, it checks the access list. If the check fails, the HTTP server does not accept the request for a connection.

Examples

The following example shows how to define an access list as 20 and assign it to the HTTP server:

```
Device> 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

Command	Description
ip access-list	Assigns an ID to an access list and enters access list configuration mode.
ip http server	Enables the HTTP 1.1 server, including the Cisco web browser user interface.

ip radius source-interface

To force RADIUS to use the IP address of a specified interface for all outgoing RADIUS packets, use the **ip radius source-interface** command in global configuration mode. To prevent RADIUS from using the IP address of a specified interface for all outgoing RADIUS packets, use the no form of this command.

ip radius source-interface *interface-name* [**vrf** *vrf-name*]
no ip radius source-interface

Syntax Description

interface-name	Name of the interface that RADIUS uses for all of its outgoing packets.
vrf *vrf-name*	(Optional) Per virtual route forwarding (VRF) configuration.

Command Default

No default behavior or values.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Use this command to set the IP address of an interface to be used as the source address for all outgoing RADIUS packets. The IP address is used as long as the interface is in the *up* state. The RADIUS server can use one IP address entry for every network access client instead of maintaining a list of IP addresses. Radius uses the IP address of the interface that it is associated to, regardless of whether the interface is in the *up* or *down* state.

The **ip radius source-interface** command is especially useful in cases where the router has many interfaces and you want to ensure that all RADIUS packets from a particular router have the same IP address.

The specified interface should have a valid IP address and should be in the *up* state for a valid configuration. If the specified interface does not have a valid IP address or is in the *down* state, RADIUS selects a local IP that corresponds to the best possible route to the AAA server. To avoid this, add a valid IP address to the interface or bring the interface to the *up* state.

Use the **vrf** *vrf-name* keyword and argument to configure this command per VRF, which allows multiple 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

mac-address	Binding MAC address.
vlan *vlan-id*	Specifies the Layer 2 VLAN identification; valid values are from 1 to 4094.
ip-address	Binding IP address.
interface *interface-id*	ID of the physical interface.

Command Default

No IP source bindings are configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

You can use this command to add a static IP source binding entry only.

The **no** format deletes the corresponding IP source binding entry. It requires the exact match of all required parameter in order for the deletion to be successful. Note that each static IP binding entry is keyed by a MAC address and a VLAN number. If the command contains the existing MAC address and VLAN number, the existing binding entry is updated with the new parameters instead of creating a separate binding entry.

This example shows how to add a static IP source binding entry:

```
Device> 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

interface	The interface whose address is used as the source address for the SSH client.

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

Release	Modification
Cisco IOS XE Gibraltar 16.10.1 Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

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.

ip verify source [**mac-check**] [**tracking**]
no ip verify source

mac-check	(Optional) Enables IP source guard with MAC address verification.
tracking	(Optional) Enables IP port security to learn static IP address learning on a port.

Command Default

IP source guard is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

To enable IP source guard with source IP address filtering, use the **ip verify source** interface configuration command.

To enable IP source guard with source IP address filtering and MAC address verification, use the **ip verify source mac-check** interface configuration command.

Examples

This example shows how to enable IP source guard with source IP address filtering on an interface:

```
Device> 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:

```
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*
noipv6 access-list *access-list-name* | **client** *permit-control-packets* | **log-update** *threshold* | **role-based** *list-name*

Syntax Description

ipv6 *access-list-name*	Creates a named IPv6 ACL (up to 64 characters in length) and enters IPv6 ACL configuration mode. *access-list-name*: Name of the IPv6 access list. Names cannot contain a space or quotation mark, or begin with a numeric.
match-local-traffic	Enables matching for locally-generated traffic.
log-update threshold *threshold-in-msgs*	Determines how syslog messages are generated after the initial packet match. *threshold-in-msgs*- Number of packets generated.
role-based *list-name*	Creates a role-based IPv6 ACL.

Command Default

No IPv6 access list is defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	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.

key chain *name* **macsec**
no key chain *name* [**macsec**]

Syntax Description

name	Name of a key chain to be used to get keys.

Command Default

Key chain macsec is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

This example shows how to configure MACsec key chain to fetch a 128-bit Pre Shared Key (PSK):

```
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):

```
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 c865632acb269022447c417504a1b
f5db1c296449b52627ba01f2ba2574c2878
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

Release	Modi
Cisco IOS XE Fuji 16.9.2	This c introd

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.

Caution 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.

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

Command	Description
password encryption aes	Enables a type 6 encrypted presh

key-server

To configure MKA key-server options, use the **key-server** command in MKA-policy configuration mode. To disable MKA key-server options, use the **no** form of this command.

key-server priority *value*
no key-server priority

Syntax Description

priority *value*	Specifies the priority value of the MKA key-server.

Command Default

MKA key-server is disabled.

Command Modes

MKA-policy configuration (config-mka-policy)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Examples

The following example shows how to configure the MKA key-server:

```
Device> enable
Device# configure terminal
Device(config)# mka policy 2
Device(config-mka-policy)# key-server priority 33
```

Related Commands

Command	Description
mka policy	Configures an MKA policy.
confidentiality-offset	Sets the confidentiality offset for MACsec operations.
delay-protection	Configures MKA to use delay protection in sending MKPDU.
include-icv-indicator	Includes ICV indicator in MKPDU.
macsec-cipher-suite	Configures cipher suite for deriving SAK)
sak-rekey	Configures the SAK rekey interval.
send-secure-announcements	Configures MKA to send secure announcements in sending MKPDUs.
ssci-based-on-sci	Computes SSCI based on the SCI.
use-updated-eth-header	Uses the updated Ethernet header for ICV calculation.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The **limit address-count** command limits the number of IPv6 addresses allowed to be used on the port on which the policy is applied. Limiting the number of IPv6 addresses on a port helps limit the binding table size. The range is from 1 to 10000.

This example shows how to define an NDP policy name as policy1, 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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

This command filters details, such as anticipated success, from MAC authentication bypass (MAB) system messages. Failure messages are not filtered.

To filter verbose MAB system messages:

```
Device> 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

Command	Description
authentication logging verbose	Filters details from authentication system messages.
dot1x logging verbose	Filters details from 802.1x system messages.
mab logging verbose	Filters details from MAC authentication bypass (MAB) system me

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Use this command to allow a RADIUS server to authenticate a new user based on the host MAC address and VLAN. Use this feature on networks with the Microsoft IAS RADIUS server. The Cisco ACS ignores this command.

This example shows how to enable VLAN-ID based MAC authentication on a device:

```
Device> enable
Device# configure terminal
Device(config)# mab request format attribute 32 vlan access-vlan
Device(config)# exit
```

Related Commands

Command	Description
authentication event	Sets the action for specific authentication events.
authentication fallback	Configures a port to use web authentication as a fallback method that do not support IEEE 802.1x authentication.
authentication host-mode	Sets the authorization manager mode on a port.
authentication open	Enables or disables open access on a port.
authentication order	Sets the order of authentication methods used on a port.
authentication periodic	Enables or disables reauthentication on a port.
authentication port-control	Enables manual control of the port authorization state.
authentication priority	Adds an authentication method to the port-priority list.
authentication timer	Configures the timeout and reauthentication parameters for an 802.1x-enabled port.

Command	Description
authentication violation	Configures the violation modes that occur when a new device a port or when a new device connects to a port with the maxi of devices already connected to that port.
mab	Enables MAC-based authentication on a port.
mab eap	Configures a port to use the Extensible Authentication Protoc
show authentication	Displays information about authentication manager events or

macsec-cipher-suite

To configure cipher suite for deriving Security Association Key (SAK), use the **macsec-cipher-suite** command in MKA-policy configuration mode. To disable cipher suite for SAK, use the **no** form of this command.

macsec-cipher-suite gcm-aes-128
no macsec-cipher-suite gcm-aes-128

Syntax Description

gcm-aes-128	Configures cipher suite for deriving SAK with 128-bit encryption.

Command Default

GCM-AES-128 encryption is enabled.

Command Modes

MKA-policy configuration (config-mka-policy)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Examples

The following example shows how to configure MACsec cipher suite for deriving SAK with 128-bit encryption:

```
Device> enable
Device# configure terminal
Device(config)# mka policy 2
Device(config-mka-policy)# macsec-cipher-suite gcm-aes-128
```

Related Commands

Command	Description
mka policy	Configures an MKA policy.
confidentiality-offset	Sets the confidentiality offset for MACsec operations.
delay-protection	Configures MKA to use delay protection in sending MKPDU.
include-icv-indicator	Includes ICV indicator in MKPDU.
key-server	Configures MKA key-server options.
sak-rekey	Configures the SAK rekey interval.
send-secure-announcements	Configures MKA to send secure announcements in sending MKPDUs.
ssci-based-on-sci	Computes SSCI based on the SCI.
use-updated-eth-header	Uses the updated Ethernet header for ICV calculation.

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	Modification
Cisco IOS XE Fuji 16.9.2	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.

match {**ip address** {*namenumber*} [{*namenumber*}] [{*namenumber*}]...|**ipv6 address** {*namenumber*} [{*namenumber*}] [{*namenumber*}]...|**mac address** {*name*} [{*name*}] [{*name*}]...}
no match {**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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

You enter access-map configuration mode by using the **vlan access-map** global configuration command.

You must enter one access list name or number; others are optional. You can match packets against one or more access lists. Matching any of the lists counts as a match of the entry.

In access-map configuration mode, use the **match** command to define the match conditions for a VLAN map applied to a VLAN. Use the **action** command to set the action that occurs when the packet matches the conditions.

Packets are matched only against access lists of the same protocol type; IP packets are matched against IP access lists, IPv6 packets are matched against IPv6 access lists, and all other packets are matched against MAC access lists.

IP, IPv6, and MAC addresses can be specified for the same map entry.

Examples

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.

mka pre-shared-key key-chain *key-chain-name*
no mka pre-shared-key key-chain *key-chain-name*

Syntax Description

mka pre-shared-key key-chain	Enables MACsec MKA configuration on device interfaces using a PSK.

Command Default

MKA pre-shared-key is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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 kc1
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 suppres syslogs sak-rekey
no mka suppres 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

Release	Modification
Cisco IOS XE Gibraltar 16.9.1	This command was introduced.

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 show 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

Release	Modifica
Cisco IOS XE Fuji 16.9.2	This com introduce

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
```

Related Commands

Command	Description
key config-key password-encrypt	Stores a type 6 encryption key

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.

{**permit** {**any** | **host***src-MAC-addr* | *src-MAC-addr mask*} {**any** | **host***dst-MAC-addr* | *dst-MAC-addr mask*} [*type mask* | **aarp** | **amber** | **appletalk** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042** | **lat** | **lavc-sca** | **lsap***lsap mask* | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** | **vines-ip** | **xns-idp**] [**cos***cos*]
nopermit {**any** | **host** *src-MAC-addr* | *src-MAC-addr mask*} {**any** | **host** *dst-MAC-addr* | *dst-MAC-addr mask*} [*type mask* | **aarp** | **amber** | **appletalk** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042** | **lat** | **lavc-sca** | **lsap** *lsap mask* | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** | **vines-ip** | **xns-idp**] [**cos***cos*]

Syntax Description

any	Denies any source or destination MAC address.
host *src-MAC-addr* | *src-MAC-addr mask*	Specifies a host MAC address and optional subnet mask. defined address, non-IP traffic from that address is denie
host *dst-MAC-addr* | *dst-MAC-addr mask*	Specifies a destination MAC address and optional subnet matches the defined address, non-IP traffic to that addres
type mask	(Optional) Specifies the EtherType number of a packet w 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 Ethe
aarp	(Optional) Specifies EtherType AppleTalk Address Reso to a network address.
amber	(Optional) Specifies EtherType DEC-Amber.
appletalk	(Optional) Specifies EtherType AppleTalk/EtherTalk.
dec-spanning	(Optional) Specifies EtherType Digital Equipment Corpo
decnet-iv	(Optional) Specifies EtherType DECnet Phase IV protoc
diagnostic	(Optional) Specifies EtherType DEC-Diagnostic.
dsm	(Optional) Specifies EtherType DEC-DSM.
etype-6000	(Optional) Specifies EtherType 0x6000.
etype-8042	(Optional) Specifies EtherType 0x8042.
lat	(Optional) Specifies EtherType DEC-LAT.
lavc-sca	(Optional) Specifies EtherType DEC-LAVC-SCA.

lsap *lsap-number mask*	(Optional) Specifies the LSAP number (0 to 65535) o the protocol of the packet. The *mask* is a mask of don't care bits applied to the L
mop-console	(Optional) Specifies EtherType DEC-MOP Remote C
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
vines-echo	(Optional) Specifies EtherType Virtual Integrated Netw
vines-ip	(Optional) Specifies EtherType VINES IP.
xns-idp	(Optional) Specifies EtherType Xerox Network Syste
cos *cos*	(Optional) Specifies an arbitrary class of service (CoS CoS can be performed only in hardware. A warning m

Command Default

This command has no defaults. However, the default action for a MAC-named ACL is to deny.

Command Modes

MAC-access list configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Though visible in the command-line help strings, **appletalk** is not supported as a matching condition.

You enter MAC access-list configuration mode by using the **mac access-list extended** global configuration command.

If you use the **host** keyword, you cannot enter an address mask; if you do not use the **any** or **host** keywords, you must enter an address mask.

After an access control entry (ACE) is added to an access control list, an implied **deny-any-any** condition exists at the end of the list. That is, if there are no matches, the packets are denied. However, before the first ACE is added, the list permits all packets.

To filter IPX traffic, you use the *type mask* or **lsap** *lsap mask* keywords, depending on the type of IPX encapsulation being used. Filter criteria for IPX encapsulation types as specified in Novell terminology and Cisco IOS XE terminology are listed in the following table.

Table 139: IPX Filtering Criteria

IPX Encapsulation Type		Filter Criterion
Cisco IOS Name	**Novell Name**	
arpa	Ethernet II	EtherType 0x8137

IPX Encapsulation Type		Filter Criterion
Cisco IOS Name	**Novell Name**	
snap	Ethernet-snap	EtherType 0x8137
sap	Ethernet 802.2	LSAP 0xE0E0
novell-ether	Ethernet 802.3	LSAP 0xFFFF

This example shows how to define the MAC-named extended access list to allow NetBIOS traffic from any source to MAC address 00c0.00a0.03fa. Traffic matching this list is allowed.

```
Device> 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

Command	Description
deny	Denies from the MA non-IP traffic to be fo
mac access-list extended	Creates an access list traffic.
show access-lists	Displays access contr

protocol (IPv6 snooping)

s

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	Modification
Cisco IOS XE Fuji 16.9.2	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
```

radius server

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

address {ipv4 | ipv6} *ip{address | hostname}*	Specifies the IP address of the RADIUS server.
auth-port *udp-port*	(Optional) Specifies the UDP port for the RADIUS authentication server. The range is from 0 to 65536.
acct-port *udp-port*	(Optional) Specifies the UDP port for the RADIUS accounting server. The range is from 0 to 65536.
key *string*	(Optional) Specifies the authentication and encryption key for all RADIUS communication between the device and the RADIUS daemon. **Note** The key is a text string that must match the encryption key used on the RADIUS server. Always configure the key as the last item in this command. Leading spaces are ignored, but spaces within and at the end of the key are used. If there are spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key.
automate tester *name*	(Optional) Enables automatic server testing of the RADIUS server status, and specify the username to be used.
retransmit *value*	(Optional) Specifies the number of times a RADIUS request is resent when the server is not responding or responding slowly. The range is 1 to 100. This setting overrides the radius-server retransmit global configuration command setting.
timeout *seconds*	(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.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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
```

radius-server dead-criteria

To force one or both of the criteria, used to mark a RADIUS server as dead, to be the indicated constant, use the **radius-server dead-criteria** command in global configuration mode. To disable the criteria that were set, use the **no** form of this command.

radius-server dead-criteria [**time** *seconds*] [**tries** *number-of-tries*]
no radius-server dead-criteria [{**time** *seconds* | **tries** *number-of-tries*}]

Syntax Description

time *seconds*	(Optional) Minimum amount of time, in seconds, that must elapse from the time that the device last received a valid packet from the RADIUS server to the time the server is marked as dead. If a packet has not been received since the device booted, and there is a timeout, the time criterion will be treated as though it has been met. You can configure the time to be from 1 through 120 seconds. • If the *seconds* argument is not configured, the number of seconds will range from 10 to 60 seconds, depending on the transaction rate of the server. **Note** Both the time criterion and the tries criterion must be met for the server to be marked as dead.
tries *number-of-tries*	(Optional) Number of consecutive timeouts that must occur on the device before the RADIUS server is marked as dead. If the server performs both authentication and accounting, both types of packets will be included in the number. Improperly constructed packets will be counted as though they were timeouts. All transmissions, including the initial transmit and all retransmits, will be counted. You can configure the number of timeouts to be from 1 through 100. • If the *number-of-tries* argument is not configured, the number of consecutive timeouts will range from 10 to 100, depending on the transaction rate of the server and the number of configured retransmissions. **Note** Both the time criterion and the tries criterion must be met for the server to be marked as dead.

Command Default

The number of seconds and number of consecutive timeouts that occur before the RADIUS server is marked as dead will vary, depending on the transaction rate of the server and the number of configured retransmissions.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Note Both the time criterion and the tries criterion must be met for the server to be marked as dead.

The **no** form of this command has the following cases:

- If neither the *seconds* nor the *number-of-tries* argument is specified with the **no radius-server dead-criteria** command, both time and tries will be reset to their defaults.
- If the *seconds* argument is specified using the originally set value, the time will be reset to the default value range (10 to 60).
- If the *number-of-tries* argument is specified using the originally set value, the number of tries will be reset to the default value range (10 to 100).

Examples

The following example shows how to configure the device so that it will be considered dead after 5 seconds and 4 tries:

```
Device> enable
Device# configure terminal
Device(config)# radius-server dead-criteria time 5 tries 4
```

The following example shows how to disable the time and number-of-tries criteria that were set for the **radius-server dead-criteria** command.

```
Device(config)# no radius-server dead-criteria
```

The following example shows how to disable the time criterion that was set for the **radius-server dead-criteria** command.

```
Device(config)# no radius-server dead-criteria time 5
```

The following example shows how to disable the number-of-tries criterion that was set for the **radius-server dead-criteria** command.

```
Device(config)# no radius-server dead-criteria tries 4
```

Related Commands

Command	Description
debug aaa dead-criteria transactions	Displays AAA dead-criteria transaction values.
show aaa dead-criteria	Displays dead-criteria information for a AAA server.
show aaa server-private	Displays the status of all private RADIUS servers.
show aaa servers	Displays information about the number of packets sent to and received from AAA servers.

radius-server deadtime

To improve RADIUS response time when some servers might be unavailable and to skip unavailable servers immediately, use the **radius-server deadtime** command in global configuration mode. To set deadtime to 0, use the **no** form of this command.

radius-server deadtime *minutes*
no radius-server deadtime

Syntax Description

minutes	Length of time, in minutes (up to a maximum of 1440 minutes or 24 hours), for which a RADIUS server is skipped over by transaction requests.

Command Default

Dead time is set to 0.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Use this command to enable the Cisco IOS software to mark as *dead* any RADIUS servers that fail to respond to authentication requests, thus avoiding the wait for the request to time out before trying the next configured server. A RADIUS server marked as *dead* is skipped by additional requests for the specified duration (in minutes) or unless there are no servers not marked as *dead*.

Note If a RADIUS server that is marked as *dead* receives a directed-request, the directed- request is not omitted by the RADIUS server. The RADIUS server continues to process the directed-request because the request is directly sent to the RADIUS server.

The RADIUS server will be marked as dead if both of the following conditions are met:

1. A valid response has not been received from the RADIUS server for any outstanding transaction for at least the timeout period that is used to determine whether to retransmit to that server, and
2. At at least the requisite number of retransmits plus one (for the initial transmission) have been sent consecutively across all transactions being sent to the RADIUS server without receiving a valid response from the server within the requisite timeout.

Examples

The following example specifies five minutes of deadtime for RADIUS servers that fail to respond to authentication requests:

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# radius-server deadtime 5
```

Related Commands

Command	Description
deadtime (server-group configuration)	Configures deadtime within the context of RADIUS server groups.
radius-server host	Specifies a RADIUS server host.
radius-server retransmit	Specifies the number of times that the Cisco IOS software searches the list of RADIUS server hosts before giving up.
radius-server timeout	Sets the interval for which a device waits for a server host to reply.

radius-server directed-request

To allow users to log in to a Cisco network access server (NAS) and select a RADIUS server for authentication, use the **radius-server directed-request** command in global configuration mode. To disable the directed-request function, use the **no** form of this command.

radius-server directed-request [**restricted**]
no radius-server directed-request [**restricted**]

Syntax Description

restricted	(Optional) Prevents the user from being sent to a secondary server if the specified server is not available.

Command Default

The User cannot log in to a Cisco NAS and select a RADIUS server for authentication.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The **radius-server directed-request** command sends only the portion of the username before the "@" symbol to the host specified after the "@" symbol. In other words, with this command enabled, you can direct a request to any of the configured servers, and only the username is sent to the specified server.

Note If a private RADIUS server is used as the group server by configuring the **server-private** (RADIUS) command, then the **radius-server directed-request** command cannot be configured.

The following is the sequence of events to send a message to RADIUS servers:

- If the **radius-server directed-request** command is configured:
  - A request is sent to the directed server. If there are more servers with the same IP address, the request is sent only to the first server with same IP address.
  - If a response is not received, requests will be sent to all servers listed in the first method list.
  - If no response is received with the first method, the request is sent to all servers listed in the second method list until the end of the method list is reached.

Note To select the directed server, search the first server group in the method list for a server with the IP address provided in a directed request. If it is not available, the first server group with the same IP address from the global pool is considered.

- If the **radius-server directed-request restricted** command is configured for every server group in the method list, until the response is received from the directed server or the end of method list is reached, the following actions occur:
  - The first server with an IP address of the directed server will be used to send the request.
  - If a server with the same IP address is not found in the server group, then the first server in the global pool with the IP address of the directed-server will be used.

If the **radius-server directed-request** command is disabled using the **no radius-server directed-request** command, the entire string, both before and after the "@" symbol, is sent to the default RADIUS server. The router queries the list of servers, starting with the first one in the list. It sends the whole string, and accepts the first response from the server.

Use the **radius-server directed-request restricted** command to limit the user to the RADIUS server identified as part of the username.

If the user request has a server IP address, then the directed server forwards it to a specific server before forwarding it to the group. For example, if a user request such as user@10.0.0.1 is sent to the directed server, and if the IP address specified in this user request is the IP address of a server, the directed server forwards the user request to the specific server.

If a directed server is configured both on the server group and on the host server, and if the user request with the configured server name is sent to the directed server, the directed server forwards the user request to the host server before forwarding it to the server group. For example, if a user request of user@10.0.0.1 is sent to the directed server and 10.0.0.1 is the host server address, then the directed server forwards the user request to the host server before forwarding the request to the server group.

Note When the **no radius-server directed-request restricted** command is entered, only the restricted flag is removed, and the directed-request flag is retained. To disable the directed-request function, you must also enter the **no radius-server directed-request** command.

Examples

The following example shows how to configure the directed-request function:

```
Device> enable
Device# configure terminal
Device(config)# radius server rad-1
Device(config-radius-server)# address ipv4 10.1.1.2
Device(config-radius-server)# key dummy123
Device(config-radius-server)# exit
Device(config)# radius-server directed-request
```

Related Commands

Command	Description
aaa group server	Groups different server hosts into distinct lists and distinct methods.
aaa new-model	Enables the AAA access control model.
server-private (**RADIUS**)	Configures the IP address of the private RADIUS server for the group server.

radius-server domain-stripping

To configure a network access server (NAS) to strip suffixes, or to strip both suffixes and prefixes from the username before forwarding the username to the remote RADIUS server, use the **radius-server domain-stripping** command in global configuration mode. To disable a stripping configuration, use the **no** form of this command.

Note The **ip vrf default** command must be configured in global configuration mode before the **radius-server domain-stripping** command is configured to ensure that the default VRF name is a NULL value until the defaulf vrf name is configured.

radius-server domain-stripping [{ [**right-to-left**] [**prefix-delimiter** *character* [*character2* . . . *character7*]] [**delimiter** *character* [*character2* . . . *character7*]] | **strip-suffix** *suffix* }] [**vrf** *vrf-name*]
no radius-server domain-stripping [{ [**right-to-left**] [**prefix-delimiter** *character* [*character2* . . . *character7*]] [**delimiter** *character* [*character2* . . . *character7*]] | **strip-suffix** *suffix* }] [**vrf** *vrf-name*]

Syntax Description

right-to-left	(Optional) Specifies that the NAS will apply the stripping configuration at the first delimiter found when parsing the full username from right to left. The default is for the NAS to apply the stripping configuration at the first delimiter found when parsing the full username from left to right.
prefix-delimiter *character* [*character2...character7*]	(Optional) Enables prefix stripping and specifies the character or characters that will be recognized as a prefix delimiter. Valid values for the *character* argument are @, /, $, %, \, #, and -. Multiple characters can be entered without intervening spaces. Up to seven characters can be defined as prefix delimiters, which is the maximum number of valid characters. If a \ is entered as the final or only value for the *character* argument, it must be entered as \\. No prefix delimiter is defined by default.
delimiter *character* [*character2...character7*]	(Optional) Specifies the character or characters that will be recognized as a suffix delimiter. Valid values for the *character* argument are @, /, $, %, \, #, and -. Multiple characters can be entered without intervening spaces. Up to seven characters can be defined as suffix delimiters, which is the maximum number of valid characters. If a \ is entered as the final or only value for the *character* argument, it must be entered as \\. The default suffix delimiter is the @ character.
strip-suffix *suffix*	(Optional) Specifies a suffix to strip from the username.
vrf *vrf-name*	(Optional) Restricts the domain stripping configuration to a Virtual Private Network (VPN) routing and forwarding (VRF) instance. The *vrf-name*argument specifies the name of a VRF.

Command Default

Stripping is disabled. The full username is sent to the RADIUS server.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Use the **radius-server domain-stripping** command to configure the NAS to strip the domain from a username before forwarding the username to the RADIUS server. If the full username is user1@cisco.com, enabling the **radius-server domain-stripping** command results in the username "user1" being forwarded to the RADIUS server.

Use the **right-to-left** keyword to specify that the username should be parsed for a delimiter from right to left, rather than from left to right. This allows strings with two instances of a delimiter to strip the username at either delimiter. For example, if the username is user@cisco.com@cisco.net, the suffix could be stripped in two ways. The default direction (left to right) would result in the username "user" being forwarded to the RADIUS server. Configuring the **right-to-left** keyword would result in the username "user@cisco.com" being forwarded to the RADIUS server.

Use the **prefix-delimiter** keyword to enable prefix stripping and to specify the character or characters that will be recognized as a prefix delimiter. The first configured character that is parsed will be used as the prefix delimiter, and any characters before that delimiter will be stripped.

Use the **delimiter** keyword to specify the character or characters that will be recognized as a suffix delimiter. The first configured character that is parsed will be used as the suffix delimiter, and any characters after that delimiter will be stripped.

Use **strip-suffix** *suffix* to specify a particular suffix to strip from usernames. For example, configuring the **radius-server domain-stripping strip-suffix cisco.net** command would result in the username user@cisco.net being stripped, while the username user@cisco.com will not be stripped. You may configure multiple suffixes for stripping by issuing multiple instances of the **radius-server domain-stripping** command. The default suffix delimiter is the @ character.

Note Issuing the **radius-server domain-stripping s trip-suffix** *suffix* command disables the capacity to strip suffixes from all domains. Both the suffix delimiter and the suffix must match for the suffix to be stripped from the full username. The default suffix delimiter of @ will be used if you do not specify a different suffix delimiter or set of suffix delimiters using the **delimiter**keyword.

To apply a domain-stripping configuration only to a specified VRF, use the **vrf** *vrf-name* option.

The interactions between the different types of domain stripping configurations are as follows:

- You may configure only one instance of the **radius-server domain-stripping**[**right-to-left**] [**prefix-delimiter** *character* [*character2...character7*]] [**delimiter** *character* [*character2...character7*]] command.
- You may configure multiple instances of the **radius-server domain-stripping**[**right-to-left**] [**prefix-delimiter** *character* [*character2...character7*]] [**delimiter** *character* [*character2...character7*]] [**vrf** *vrf-name*] command with unique values for **vrf** *vrf-name*.
- You may configure multiple instances of the **radius-server domain-stripping strip-suffix** *suffix*[**vrf** *per-vrf*] command to specify multiple suffixes to be stripped as part of a global or per-VRF ruleset.

- Issuing any version of the **radius-server domain-stripping** command automatically enables suffix stripping using the default delimiter character @ for that ruleset, unless a different delimiter or set of delimiters is specified.
- Configuring a per-suffix stripping rule disables generic suffix stripping for that ruleset. Only suffixes that match the configured suffix or suffixes will be stripped from usernames.

Examples

The following example configures the router to parse the username from right to left and sets the valid suffix delimiter characters as @, \, and $. If the full username is cisco/user@cisco.com$cisco.net, the username "cisco/user@cisco.com" will be forwarded to the RADIUS server because the $ character is the first valid delimiter encountered by the NAS when parsing the username from right to left.

```
radius-server domain-stripping right-to-left delimiter @\$
```

The following example configures the router to strip the domain name from usernames only for users associated with the VRF instance named abc. The default suffix delimiter @ will be used for generic suffix stripping.

```
radius-server domain-stripping vrf abc
```

The following example enables prefix stripping using the character / as the prefix delimiter. The default suffix delimiter character @ will be used for generic suffix stripping. If the full username is cisco/user@cisco.com, the username "user" will be forwarded to the RADIUS server.

```
radius-server domain-stripping prefix-delimiter /
```

The following example enables prefix stripping, specifies the character / as the prefix delimiter, and specifies the character # as the suffix delimiter. If the full username is cisco/user@cisco.com#cisco.net, the username "user@cisco.com" will be forwarded to the RADIUS server.

```
radius-server domain-stripping prefix-delimiter / delimiter #
```

The following example enables prefix stripping, configures the character / as the prefix delimiter, configures the characters $, @, and # as suffix delimiters, and configures per-suffix stripping of the suffix cisco.com. If the full username is cisco/user@cisco.com, the username "user" will be forwarded to the RADIUS server. If the full username is cisco/user@cisco.com#cisco.com, the username "user@cisco.com" will be forwarded.

```
radius-server domain-stripping prefix-delimiter / delimiter $@#
radius-server domain-stripping strip-suffix cisco.com
```

The following example configures the router to parse the username from right to left and enables suffix stripping for usernames with the suffix cisco.com. If the full username is cisco/user@cisco.net@cisco.com, the username "cisco/user@cisco.net" will be forwarded to the RADIUS server. If the full username is cisco/user@cisco.com@cisco.net, the full username will be forwarded.

```
radius-server domain-stripping right-to-left
radius-server domain-stripping strip-suffix cisco.com
```

The following example configures a set of global stripping rules that will strip the suffix cisco.com using the delimiter @, and a different set of stripping rules for usernames associated with the VRF named myvrf:

```
radius-server domain-stripping strip-suffix cisco.com
!
radius-server domain-stripping prefix-delimiter # vrf myvrf
radius-server domain-stripping strip-suffix cisco.net vrf myvrf
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.
ip vrf	Defines a VRF instance and enters VRF configuration mode.
tacacs-server domain-stripping	Configures a router to strip a prefix or suffix from the username before forwarding the username to the TACACS+ server.

sak-rekey

To configure the Security Association Key (SAK) rekey time interval for a defined MKA policy, use the **sak-rekey** command in MKA-policy configuration mode. To stop the SAK rekey timer, use the **no** form of this command.

sak-rekey {**interval** *time-interval* | **on-live-peer-loss**}
no sak-rekey {**interval** | **on-live-peer-loss**}

Syntax Description

interval *time-interval*	SAK rekey interval in seconds. The range is from 30 to 65535, and the default is 0.
on-live-peer-loss	Peer loss from the live membership.

Command Default

The SAK rekey timer is disabled. The default is 0.

Command Modes

MKA-policy configuration (config-mka-policy)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Examples

The following example shows how to configure the SAK rekey interval:

```
Device> enable
Device# configure terminal
Device(config)# mka policy 2
Device(config-mka-policy)# sak-rekey interval 300
```

Related Commands

Command	Description
mka policy	Configures an MKA policy.
confidentiality-offset	Sets the confidentiality offset for MACsec operations.
delay-protection	Configures MKA to use delay protection in sending MKPDU.
include-icv-indicator	Includes ICV indicator in MKPDU.
key-server	Configures MKA key-server options.
macsec-cipher-suite	Configures cipher suite for deriving SAK.
send-secure-announcements	Configures MKA to send secure announcements in sending MKPDUs.
ssci-based-on-sci	Computes SSCI based on the SCI.
use-updated-eth-header	Uses the updated Ethernet header for ICV calculation.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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
```

send-secure-announcements

To enable MKA to send secure announcements in MACsec Key Agreement Protocol Data Units (MKPDUs), use the **send-secure-announcements** command in MKA-policy configuration mode. To disable sending of secure announcements, use the **no** form of this command.

send-secure-announcements
no send-secure-announcements

Syntax Description

This command has no arguments or keywords.

Command Default

Secure announcements in MKPDUs is disabled.

Command Modes

MKA-policy configuration (config-mka-policy)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Secure announcements revalidate the MACsec Cipher Suite capabilities which were shared previously through unsecure announcements.

Examples

The following example shows how to enable sending of secure announcements:

```
Device> enable
Device# configure terminal
Device(config)# mka policy 2
Device(config-mka-policy)# send-secure-announcements
```

Related Commands

Command	Description
mka policy	Configures an MKA policy.
confidentiality-offset	Sets the confidentiality offset for MACsec operations.
delay-protection	Configures MKA to use delay protection in sending MKPDU.
include-icv-indicator	Includes ICV indicator in MKPDU.
key-server	Configures MKA key-server options.
macsec-cipher-suite	Configures cipher suite for deriving SAK.
sak-rekey	Configures the SAK rekey interval.
ssci-based-on-sci	Computes SSCI based on the SCI.
use-updated-eth-header	Uses the updated ethernet header for ICV calculation.

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

ip-address	IP address of the private RADIUS server host.
auth-port *port-number*	(Optional) User Datagram Protocol (UDP) destination port for authentication requests. The default value is 1645.
acct-port *port-number*	Optional) UDP destination port for accounting requests. The default value is 1646.
non-standard	(Optional) RADIUS server is using vendor-proprietary RADIUS attributes.
timeout *seconds*	(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 **radius-server timeout** command. If no timeout value is specified, the global value is used.
retransmit *retries*	(Optional) Number of times a RADIUS request is resent to a server, if that server is not responding or responding slowly. This setting overrides the global setting of the **radius-server retransmit** command.
key *string*	(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 **radius-server key** command. If no key string is specified, the global value is used. The *string* can be **0** (specifies that an unencrypted key follows), **6** (specifies that an advanced encryption scheme [AES] encrypted key follows), **7** (specifies that a hidden key follows), or a line specifying the unencrypted (clear-text) server key.

Command Default

If server-private parameters are not specified, global configurations will be used; if global configurations are not specified, default values will be used.

Command Modes

RADIUS server-group configuration (config-sg-radius)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Use the **server-private** command to associate a particular private server with a defined server group. To prevent possible overlapping of private addresses between virtual route forwarding (VRF) instances, private

servers (servers with private addresses) can be defined within the server group and remain hidden from other groups, while the servers in the global pool (default "radius" server group) can still be referred to by IP addresses and port numbers. Thus, the list of servers in server groups includes references to the hosts in the global configuration and the definitions of private servers.

Note

- If the **radius-server directed-request** command is configured, then a private RADIUS server cannot be used as the group server by configuring the **server-private** (RADIUS) command.
- Creating or updating AAA server statistics record for private RADIUS servers are not supported. If private RADIUS servers are used, then error messages and tracebacks will be encountered, but these error messages or tracebacks do not have any impact on the AAA RADIUS functionality. To avoid these error messages and tracebacks, configure public RADIUS server instead of private RADIUS server.

Use the **password encryption aes** command to configure type 6 AES encrypted keys.

Examples

The following example shows how to define the sg_water RADIUS group server and associate private servers with it:

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa group server radius sg_water
Device(config-sg-radius)# server-private 10.1.1.1 timeout 5 retransmit 3 key xyz
Device(config-sg-radius)# server-private 10.2.2.2 timeout 5 retransmit 3 key xyz
Device(config-sg-radius)# end
```

Related Commands

Command	Description
aaa group server	Groups different server hosts into distinct lists and distinct methods.
aaa new-model	Enables the AAA access control model.
password encryption aes	Enables a type 6 encrypted preshared key.
radius-server host	Specifies a RADIUS server host.
radius-server directed-request	Allows users to log in to a Cisco NAS and select a RADIUS server for authentication.

server-private (TACACS+)

To configure the IPv4 or IPv6 address of the private TACACS+ server for the group server, use the **server-private** command in 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 { *ipv4-address* | *ipv6-address* | **fqdn** } [**nat**] [**single-connection**] [**port** *port-number*] [**timeout** *seconds*] **key** [{ **0** | **7** }] *string*
no server-private

Syntax Description

ip4-address	IPv4 address of the private TACACS+ server host.
ip6-address	IPv6 address of the private TACACS+ server host.
fqdn	Fully qualified domain name (fqdn) of the private TACACS+ server host for address resolution from the Domain Name Server (DNS)
nat	(Optional) Specifies the port Network Address Translation (NAT) address of the remote device. This address is sent to the TACACS+ server.
single-connection	(Optional) Maintains a single TCP connection between the router and the TACACS+ server.
timeout *seconds*	(Optional) Specifies a timeout value for the server response. This value overrides the global timeout value set with the **tacacs-server timeout** command for this server only.
port *port-number*	(Optional) Specifies a server port number. This option overrides the default, which is port 49.
key [**0** | **7**] *string*	(Optional) Specifies an authentication and encryption key. This key must match the key used by the TACACS+ daemon. Specifying this key overrides the key set by the global tacacs-server key command for this server only. If no number or 0 is entered, the *string* that is entered is considered to be plain text. If 7 is entered, the *string* that is entered is considered to be encrypted text.

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

TACACS+ server-group configuration (config-sg-tacacs+)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Use the **server-private** command to associate a particular private server with a defined server group. To prevent possible overlapping of private addresses between virtual route forwardings (VRFs), 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 "TACACS+" 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.

The following example shows how to define the tacacs1 TACACS+ group server and associate private servers with it:

```
Device> enable
Device# configure terminal
Device(config)# aaa group server tacacs+ tacacs1
Device(config-sg-tacacs+)# server-private 10.1.1.1 port 19 key cisco
Device(config-sg-tacacs+)# exit
Device(config)#ip vrf cisco
Device(config-vrf)# rd 100:1
Device(config-vrf)# exit
Device(config)# interface Loopback0
Device(config-if)#ip address 10.0.0.2 255.0.0.0
Device(config-if)#ip vrf forwarding cisco
```

Related Commands

Command	Description
aaa group server	Groups different server hosts into distinct lists and distinct methods.
aaa new-model	Enables the AAA access control model.
ip tacacs source-interface	Uses the IP address of a specified interface for all outgoing TACACS+ packets.
ip vrf forwarding (server-group)	Configures the VRF reference of an AAA TACACS+ server group.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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 aruguments or keywords.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

This is an example of output from the **show aaa command handler** command:

```
Device# show aaa command handler

AAA Command Handler Statistics:
    account-logon: 0, account-logoff: 0
    account-query: 0, pod: 0
    service-logon: 0, service-logoff: 0
    user-profile-push: 0, session-state-log: 0
    reauthenticate: 0, bounce-host-port: 0
    disable-host-port: 0, update-rbacl: 0
    update-sgt: 0, update-cts-policies: 0
    invalid commands: 0
    async message not sent: 0
```

show aaa dead-criteria

To display dead-criteria detection information for an authentication, authorization, and accounting (AAA) server, use the **show aaa dead-criteria** command in privileged EXEC mode.

show aaa dead-criteria {**security-protocol** *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*][*server-group-name*]

Syntax Description

security-protocol	Security protocol of the specified AAA server. Currently, the only protocol that is supported is RADIUS.
ip-address	IP address of the specified AAA server.
auth-port	(Optional) Authentication port for the RADIUS server that was specified.
port-number	(Optional) Number of the authentication port. The default is 1645 (for a RADIUS server).
acct-port	(Optional) Accounting port for the RADIUS server that was specified.
port-number	(Optional) Number of the accounting port. The default is 1646 (for a RADIUS server).
server-group-name	(Optional) Server group with which the specified server is associated. The default is *radius* (for a RADIUS server).

Command Default

Currently, the *port-number* argument for the **auth-port** keyword and the *port-number* argument for the **acct-port** keyword default to 1645 and 1646, respectively. The default for the *server-group-name* argument is radius.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Multiple RADIUS servers having the same IP address can be configured on a device. The **auth-port** and **acct-port** keywords are used to differentiate the servers. The dead-detect interval of a server that is associated with a specified server group can be obtained by using the **server-group-name** keyword. (The dead-detect interval and retransmit values of a RADIUS server are set on the basis of the server group to which the server belongs. The same server can be part of multiple server groups.)

Examples

The following example shows that dead-criteria-detection information has been requested for a RADIUS server at the IP address 172.19.192.80:

```
Device# show aaa dead-criteria radius 172.19.192.80 radius

RADIUS Server Dead Critieria:
=============================
Server Details:
    Address : 172.19.192.80
```

```
    Auth Port : 1645
    Acct Port : 1646
Server Group : radius
Dead Criteria Details:
    Configured Retransmits : 62
    Configured Timeout : 27
    Estimated Outstanding Transactions: 5
    Dead Detect Time : 25s
    Computed Retransmit Tries: 22
    Statistics Gathered Since Last Successful Transaction
=====================================================
Max Computed Outstanding Transactions: 5
Max Computed Dead Detect Time: 25s
Max Computed Retransmits : 22
```

The **Max Computed Dead Detect Time** is displayed in seconds. The other fields shown in the display are self-explanatory.

Related Commands

Command	Description
debug aaa dead-criteria transactions	Displays AAA dead-criteria transaction values.
radius-server dead-criteria	Forces one or both of the criteria, used to mark a RADIUS server as dead, to be the indicated constant.
show aaa server-private	Displays the status of all private RADIUS servers.
show aaa servers	Displays information about the number of packets sent to and received from AAA servers.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

This is an example of output from the **show aaa local statistics** command:

```
Device# show aaa local statistics

Local EAP statistics

EAP Method         Success       Fail
---------------------------------------
Unknown                  0          0
EAP-MD5                  0          0
EAP-GTC                  0          0
LEAP                     0          0
PEAP                     0          0
EAP-TLS                  0          0
EAP-MSCHAPV2             0          0
EAP-FAST                 0          0

Requests received from AAA:                  0
Responses returned from EAP:                 0
Requests dropped (no EAP AVP):               0
Requests dropped (other reasons):            0
Authentication timeouts from EAP:            0

Credential request statistics
Requests sent to backend:                    0
Requests failed (unable to send):            0
Authorization results received

  Success:                                   0
```

```
Fail:                                    0
```

show aaa servers

To 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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Examples

The following is a sample output from the **show aaa servers** command:

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

The following is a sample output from the **show authentication brief** command:

```
Device# show authentication brief

Interface  MAC Address     AuthC           AuthZ                    Fg  Uptime
-------------------------------------------------------------------------------
Gi2/0/14   0002.0002.0001  m:NA d:OK      AZ: SA-                   X     281s
Gi2/0/14   0002.0002.0002  m:NA d:OK      AZ: SA-                   X     280s
Gi2/0/14   0002.0002.0003  m:NA d:OK      AZ: SA-                   X     279s
Gi2/0/14   0002.0002.0004  m:NA d:OK      AZ: SA-                   X     278s
Gi2/0/14   0002.0002.0005  m:NA d:OK      AZ: SA-                   X     278s
Gi2/0/14   0002.0002.0006  m:NA d:OK      AZ: SA-                   X     277s
Gi2/0/14   0002.0002.0007  m:NA d:OK      AZ: SA-                   X     276s
Gi2/0/14   0002.0002.0008  m:NA d:OK      AZ: SA-                   X     276s
Gi2/0/14   0002.0002.0009  m:NA d:OK      AZ: SA-                   X     275s
Gi2/0/14   0002.0002.000a  m:NA d:OK      AZ: SA-                   X     275s
Gi2/0/14   0002.0002.000b  m:NA d:OK      AZ: SA-                   X     274s
Gi2/0/14   0002.0002.000c  m:NA d:OK      AZ: SA-                   X     274s
Gi2/0/14   0002.0002.000d  m:NA d:OK      AZ: SA-                   X     273s
Gi2/0/14   0002.0002.000e  m:NA d:OK      AZ: SA-                   X     273s
Gi2/0/14   0002.0002.000f  m:NA d:OK      AZ: SA-                   X     272s
Gi2/0/14   0002.0002.0010  m:NA d:OK      AZ: SA-                   X     272s
Gi2/0/14   0002.0002.0011  m:NA d:OK      AZ: SA-                   X     271s
Gi2/0/14   0002.0002.0012  m:NA d:OK      AZ: SA-                   X     271s
Gi2/0/14   0002.0002.0013  m:NA d:OK      AZ: SA-                   X     270s
Gi2/0/14   0002.0002.0014  m:NA d:OK      AZ: SA-                   X     270s
Gi2/0/14   0002.0002.0015  m:NA d:OK      AZ: SA-                   X     269s
```

The following is a sample output from the **show authentication brief** command for active instances:

```
Device# show authentication brief switch active R0

Interface  MAC Address     AuthC           AuthZ                    Fg  Uptime
-----------------------------------------------------------------------------
Gi2/0/14   0002.0002.0001  m:NA d:OK      AZ: SA-                   X       1s
Gi2/0/14   0002.0002.0002  m:NA d:OK      AZ: SA-                   X       0s
Gi2/0/14   0002.0002.0003  m:NA d:OK      AZ: SA-                   X     299s
Gi2/0/14   0002.0002.0004  m:NA d:OK      AZ: SA-                   X     298s
Gi2/0/14   0002.0002.0005  m:NA d:OK      AZ: SA-                   X     298s
Gi2/0/14   0002.0002.0006  m:NA d:OK      AZ: SA-                   X     297s
Gi2/0/14   0002.0002.0007  m:NA d:OK      AZ: SA-                   X     296s
Gi2/0/14   0002.0002.0008  m:NA d:OK      AZ: SA-                   X     296s
Gi2/0/14   0002.0002.0009  m:NA d:OK      AZ: SA-                   X     295s
Gi2/0/14   0002.0002.000a  m:NA d:OK      AZ: SA-                   X     295s
Gi2/0/14   0002.0002.000b  m:NA d:OK      AZ: SA-                   X     294s
Gi2/0/14   0002.0002.000c  m:NA d:OK      AZ: SA-                   X     294s
Gi2/0/14   0002.0002.000d  m:NA d:OK      AZ: SA-                   X     293s
Gi2/0/14   0002.0002.000e  m:NA d:OK      AZ: SA-                   X     293s
Gi2/0/14   0002.0002.000f  m:NA d:OK      AZ: SA-                   X     292s
Gi2/0/14   0002.0002.0010  m:NA d:OK      AZ: SA-                   X     292s
Gi2/0/14   0002.0002.0011  m:NA d:OK      AZ: SA-                   X     291s
Gi2/0/14   0002.0002.0012  m:NA d:OK      AZ: SA-                   X     291s
Gi2/0/14   0002.0002.0013  m:NA d:OK      AZ: SA-                   X     290s
Gi2/0/14   0002.0002.0014  m:NA d:OK      AZ: SA-                   X     290s
Gi2/0/14   0002.0002.0015  m:NA d:OK      AZ: SA-                   X     289s
Gi2/0/14   0002.0002.0016  m:NA d:OK      AZ: SA-                   X     289s
```

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 140: show authentication brief Field Descriptions

Field	Description
Interface	The type and number of the authentication interface.
MAC Address	The MAC address of the client.
AuthC	Indicates authentication status.
AuthZ	Indicates authorization status.

Field	Description
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 sessions

To display information about current Auth Manager sessions, use the **show authentication sessions** command.

show authentication sessions [**database**] [**handle** *handle-id* [**details**]] [**interface** *type number* [**details**] [**mac** *mac-address* [**interface** *type number*] [**method** *method-name* [**interface** *type number* [**details**] [**session-id** *session-id* [**details**]]

Syntax Description

database	(Optional) Shows only data stored in session database.
handle *handle-id*	(Optional) Specifies the particular handle for which Auth Manager information is to be displayed.
details	(Optional) Shows detailed information.
interface *type number*	(Optional) Specifies a particular interface type and number for which Auth Manager information is to be displayed.
mac *mac-address*	(Optional) Specifies the particular MAC address for which you want to display information.
method *method-name*	(Optional) Specifies the particular authentication method for which Auth Manager information is to be displayed. If you specify a method (**dot1x**, **mab**, or **webauth**), you may also specify an interface.
session-id *session-id*	(Optional) Specifies the particular session for which Auth Manager information is to be displayed.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Use the **show authentication sessions** command to display information about all current Auth Manager sessions. To display information about specific Auth Manager sessions, use one or more of the keywords.

This table shows the possible operating states for the reported authentication sessions.

Table 141: Authentication Method States

State	Description
Not run	The method has not run for this session.
Running	The method is running for this session.
Failed over	The method has failed and the next method is expected to provide a result.

State	Description
Success	The method has provided a successful authentication result for the session.
Authc Failed	The method has provided a failed authentication result for the session.

This table shows the possible authentication methods.

Table 142: Authentication Method States

State	Description
dot1x	802.1X
mab	MAC authentication bypass
webauth	web authentication

The following example shows how to display all authentication sessions on the device:

```
Device# show authentication sessions

Interface    MAC Address     Method   Domain   Status         Session ID
Gi1/0/48     0015.63b0.f676  dot1x    DATA     Authz Success  0A3462B1000000102983C05C
Gi1/0/5      000f.23c4.a401  mab      DATA     Authz Success  0A3462B10000000D24F80B58
Gi1/0/5      0014.bf5d.d26d  dot1x    DATA     Authz Success  0A3462B10000000E29811B94
```

The following example shows how to display all authentication sessions on an interface:

```
Device# show authentication sessions interface gigabitethernet2/0/47

            Interface:  GigabitEthernet2/0/47
          MAC Address:  Unknown
           IP Address:  Unknown
               Status:  Authz Success
               Domain:  DATA
      Oper host mode:  multi-host
    Oper control dir:  both
       Authorized By:  Guest Vlan
         Vlan Policy:  20
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  0A3462C8000000000002763C
     Acct Session ID:  0x00000002
              Handle:  0x25000000
Runnable methods list:
       Method   State
       mab      Failed over
       dot1x    Failed over
----------------------------------------
            Interface:  GigabitEthernet2/0/47
          MAC Address:  0005.5e7c.da05
           IP Address:  Unknown
            User-Name:  00055e7cda05
               Status:  Authz Success
```

```
               Domain:  VOICE
      Oper host mode:  multi-domain
    Oper control dir:  both
       Authorized By:  Authentication Server
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  0A3462C8000000010002A238
     Acct Session ID:  0x00000003
               Handle:  0x91000001
Runnable methods list:
      Method   State
      mab      Authc Success
      dot1x    Not run
```

show cisp

To display Client Information Signaling Protocol (CISP) information for a specified interface, use the **show cisp** command in privileged EXEC mode.

show cisp { [**clients** | **interface** *interface-id*] | **registrations** | **summary**}

Syntax Description

clients	(Optional) Display CISP client details.
interface *interface-id*	(Optional) Display CISP information about the specified inte channels.
registrations	Displays CISP registrations.
summary	(Optional) Displays CISP summary.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

The following is sample output from the **show cisp interface** command:

```
Device# show cisp interface fastethernet 0/1/1

CISP not enabled on specified interface
```

The following is sample output from the **show cisp registration** command:

```
Device# show cisp registrations

Interface(s) with CISP registered user(s):
-------------------------------------------
Fa1/0/13
Auth Mgr (Authenticator)
Gi2/0/1
Auth Mgr (Authenticator)
Gi2/0/2
Auth Mgr (Authenticator)
Gi2/0/3
Auth Mgr (Authenticator)
Gi2/0/5
Auth Mgr (Authenticator)
Gi2/0/9
Auth Mgr (Authenticator)
Gi2/0/11
Auth Mgr (Authenticator)
Gi2/0/13
Auth Mgr (Authenticator)
Gi3/0/3
Gi3/0/5
```

```
Gi3/0/23
```

Related Commands

Command	Description
cisp enable	Enables CISP.
dot1x credentials *profile*	Configures a profile on a supplicant device.

show device-tracking capture-policy

To display the rules that the system pushes to the hardware (forwarding layer), enter the **show device-tracking capture-policy** command in privileged EXEC mode. These rules determine which packets are punted to SISF for further action. These rules are a translation of the policy that is applied to the interface or VLAN.

show device-tracking capture-policy [**interface** *inteface_type_no* | **vlan** *vlan_id*]

Syntax Description

interface *inteface_type_no*	Displays message capture policy information for the interface you specify. Enter an interface type and number. Use the question mark (?) online help function to display the types of interfaces on the device.
vlan *vlan_id*	Displays message capture policy information for the VLAN ID you specify. The valid value range is from 1 to 4095.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The output of this command is used by the technical support team, for troubleshooting.

Examples

The following is sample output from the **show device-tracking capture-policy** command:

```
Device# show device-tracking capture-policy interface tengigabitethernet1/0/1

    HW Target Te1/0/1 HW policy signature 0001DF9F policies#:1 rules 14 sig 0001DF9F
        SW policy sisf-01 feature Device-tracking - Active

        Rule DHCP4 CLIENT Protocol UDP mask 00000400 action PUNT match1 0 match2 67#feat:1
            feature Device-tracking
        Rule DHCP4 SERVER SOURCE Protocol UDP mask 00001000 action PUNT match1 0 match2
68#feat:1
            feature Device-tracking
        Rule DHCP4 SERVER Protocol UDP mask 00000800 action PUNT match1 67 match2 0#feat:1
            feature Device-tracking
        Rule ARP Protocol IPV4 mask 00004000 action PUNT match1 0 match2 0#feat:1
            feature Device-tracking
        Rule DHCP SERVER SOURCE Protocol UDP mask 00000200 action PUNT match1 0 match2
546#feat:1
            feature Device-tracking
        Rule DHCP CLIENT Protocol UDP mask 00000080 action PUNT match1 0 match2 547#feat:1
            feature Device-tracking
        Rule DHCP SERVER Protocol UDP mask 00000100 action PUNT match1 547 match2 0#feat:1
            feature Device-tracking
        Rule RS Protocol ICMPV6 mask 00000004 action PUNT match1 133 match2 0#feat:1
            feature Device-tracking
        Rule RA Protocol ICMPV6 mask 00000008 action PUNT match1 134 match2 0#feat:1
```

```
    feature Device-tracking
Rule NS Protocol ICMPV6 mask 00000001 action PUNT match1 135 match2 0#feat:1
    feature Device-tracking
Rule NA Protocol ICMPV6 mask 00000002 action PUNT match1 136 match2 0#feat:1
    feature Device-tracking
Rule REDIR Protocol ICMPV6 mask 00000010 action PUNT match1 137 match2 0#feat:1
    feature Device-tracking
Rule DAR Protocol ICMPV6 mask 00008000 action PUNT match1 157 match2 0#feat:1
    feature Device-tracking
Rule DAC Protocol ICMPV6 mask 00010000 action PUNT match1 158 match2 0#feat:1
    feature Device-tracking
```

show device-tracking counters

To display information about the number of broadcast, multicast, bridged, unicast, probe, dropped device-tracking messages and faults received on an interface or VLAN or both, enter the **show device-tracking counters** command in privileged EXEC mode. Where applicable, the messages are categorized by protocol. The list of protocols include Address Resolution Protocol (ARP), Neighbor Discovery Protocol (NDP), DHCPv6, DHCPv4, Address Collision Detection (ACD), and Duplicate Address Detection (DAD).

show device-tracking counters [**all** | **interface** *inteface_type_no* | **vlan** *vlan_id*]

Syntax Description

all	Displays information for all interfaces and VLANs on the device where a policy is attached.
interface *inteface_type_no*	Displays information for the specified interface. Enter an interface type and number. Use the question mark (?) online help function to display the types of interfaces on the device.
vlan *vlan_id*	Displays information for the VLAN ID you specify. The range is from 1 to 4095.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

When you enter the **show device-tracking counters**command, you must enter one of the keywords that follow, that is, **all**, or **interface** *inteface_type_no* , or **vlan** *vlan_id* .

If you specify an interface or VLAN where a policy is not attached, the following message is displayed: `% no ipv6 snooping policy attached on <interface number or VLAN ID>`

Examples

The following is sample output from the**show device-tracking counters** command. Information relating to a particular VLAN (VLAN 10) is displayed here:

```
Device# show device-tracking counters vlan 10
Received messages on vlan 10   :
Protocol        Protocol message
NDP             RA[2479] NS[1757] NA[2794]
DHCPv6
ARP             REP[878]
DHCPv4
ACD&DAD         --[3]

Received Broadcast/Multicast messages on vlan 10   :
Protocol        Protocol message
NDP             RA[2479] NS[3] NA[5]
DHCPv6
```

```
ARP             REP[1]
DHCPv4

Bridged messages from vlan 10   :
Protocol        Protocol message
NDP             RA[1238] NS[1915] NA[878]
DHCPv6
ARP             REQ[877]
DHCPv4
ACD&DAD         --[1]

Broadcast/Multicast converted to unicast messages from vlan 10   :
Protocol        Protocol message
NDP
DHCPv6
ARP
DHCPv4
ACD&DAD

Probe message on vlan 10   :
Type            Protocol message
PROBE_SEND      NS[1037] REQ[877]
PROBE_REPLY     NA[1037] REP[877]

Limited Broadcast to Local message on vlan 10   :
Type            Protocol message
NDP
DHCPv6
ARP
DHCPv4

Dropped messages on vlan 10   :
Feature             Protocol Msg [Total dropped]
Device-tracking:    NDP      RA  [1241]
                    reason:  Packet not authorized on port [1241]

                             NS  [2]
                    reason:  Silent drop [2]

                             NA  [1039]
                    reason:  Silent drop [1037]
                    reason:  Packet accepted but not forwarded [2]

                    ARP      REP [878]
                    reason:  Silent drop [877]
                    reason:  Packet accepted but not forwarded [1]

ACD&DAD:            --       --  [2]


Faults on vlan 10   :
```

show device-tracking database

To display details of the binding table database, enter the **show device-tracking database** command in privileged EXEC mode.

show device-tracking database [**address** { *hostname_address* | **all** } [**interface** *inteface_type_no*] [**vlanid** *vlan*] [**details**] | **details** | **interface** *inteface_type_no* [**details**] [**vlanid** *vlan*] | **mac** [*48_bit_hw_add*] [**details**] [**interface** *inteface_type_no*] [**vlanid** *vlan*] | **prefix** [*prefix_address* | **all**] [**details**] [**interface** *inteface_type_no*] | **vlanid** *vlanid* [**details**]]

Syntax Description

address {*hostname_address* | **all**}	Displays binding table information for a particular IP address or for all addresses
interface *inteface_type_no*	Displays binding table information for the specified interface. Enter an interface type and number. Use the question mark (?) online help function to display the types of interfaces on the device.
vlanid *vlan*	Displays binding table information for the VLAN ID you specify. The valid value range is from 1 to 4095.
details	Displays detailed information.
mac	Displays binding table information for the MAC address you specify.
48_bit_hw_add	Enter a 48-bit hardware address.
prefix	Displays binding table information for the IPv6 prefix you specify.
prefix_address	Enter an IPv6 prefix.
all	Displays binding table information for all the available IPv6 prefixes.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Examples

The following is sample output for the **show device-tracking database details**command. The accompanying table describes the significant fields shown in the display.

```
Device# show device-tracking database details

 Binding table configuration:
 ---------------------------
 max/box  : no limit
 max/vlan : no limit
```

```
 max/port : no limit
 max/mac  : no limit

 Binding table current counters:
 -------------------------------
 dynamic  : 5
 local    : 1
 total    : 5

 Binding table counters by state:
 ---------------------------------
 REACHABLE  : 5
      DOWN  : 1
     total  : 6

Codes: L - Local, S - Static, ND - Neighbor Discovery, ARP - Address Resolution Protocol,
DH4 - IPv4 DHCP, DH6 - IPv6 DHCP, PKT - Other Packet, API - API created
Preflevel flags (prlvl):
0001:MAC and LLA match     0002:Orig trunk            0004:Orig access
0008:Orig trusted trunk    0010:Orig trusted access   0020:DHCP assigned
0040:Cga authenticated     0080:Cert authenticated    0100:Statically assigned


    Network Layer Address   Link Layer Address   Interface  mode     vlan(prim)   prlvl
age    state      Time left   Filter   In Crimson   Client ID          Session ID
Policy (feature)
ARP 192.0.9.29              001b.4411.3ab7(S)    Te1/0/4    trunk    200 ( 200)   0003
6mn    REACHABLE  331 s       no       yes          0000.0000.0000     (unspecified)
sisf-01 (Device-tracking)
ARP 192.0.9.28              001b.4411.3ab7(S)    Te1/0/4    trunk    200 ( 200)   0003
6mn    REACHABLE  313 s       no       yes          0000.0000.0000     (unspecified)
sisf-01 (Device-tracking)
ARP 192.0.9.27              001b.4411.3ab7(S)    Te1/0/4    trunk    200 ( 200)   0003
6mn    REACHABLE  323 s       no       yes          0000.0000.0000     (unspecified)
sisf-01 (Device-tracking)
ARP 192.0.9.26              001b.4411.3ab7(S)    Te1/0/4    trunk    200 ( 200)   0003
6mn    REACHABLE  311 s       no       yes          0000.0000.0000     (unspecified)
sisf-01 (Device-tracking)
ARP 192.0.9.25              001b.4411.3ab7(S)    Te1/0/4    trunk    200 ( 200)   0003
6mn    REACHABLE  313 s       no       yes          0000.0000.0000     (unspecified)
sisf-01 (Device-tracking)
L   192.168.0.1              00a5.bf9d.0462(D)      Vl200      svi    200 ( 200)   0100
6mn    DOWN                    no       yes          0000.0000.0000     (unspecified)
sisf-01 (sisf_local)
```

Table 143: show device-tracking database details Field Descriptions

Field	Description
Binding table configuration: • max/box • max/vlan • max/port • max/mac	Displays binding table settings. The values correspond with what is configured using the **device-tracking binding** command in global configuration mode. • max/box: The value displayed here corresponds with the configured value for the **max-entries** *no_of_entries* keyword. • max/vlan: The value displayed here corresponds with the configured value for the **vlan-limit** *no_of_entries* keyword. • max/port: The value displayed here corresponds with the configured value for the **port-limit** *no_of_entries* keyword. • max/mac: The value displayed here corresponds with the configured value for the **mac-limit** *no_of_entries* keyword.
Binding table current counters: • dynamic • local • total	Displays the number of entries in the table. • dynamic: Dynamic entries are created by learning events that dynamically populate the binding table. • local: Local entries are automatically created when you configure an SVI on the device. One of ways in which SISF uses a local entry, is in the context of polling. If polling is enabled, the SVI address is used as the source address of an ARP probe. • total: The total is a sum of the dynamic, local, and static binding entries.
Binding table counters by state:	Displays the number of entries in each state. The state can be REACHABLE, STALE, DOWN.
Codes	Clarifies abbreviations that are used to signify learning events. The first column of a binding entry uses an abbreviated code, which tells you about the learning event that resulted in creation of that binding entry.

Field	Description
Preflevel flags (prlvl)	A list of preference level number codes and clarification for what the number codes in the `prlvl` column of the binding table mean. The codes signify a broad classification and multiple codes can apply to an entry. What is displayed in the `prlvl` column is a sum of these number codes and signifies a corresponding preference level. For example if an ARP entry (preference code: 0001) is learned from an access interface (preference code: 0004), the value displayed in the `prlvl` column is "0005". 1 is the lowest preference level, and 100 is the highest. A binding entry with a higher preference is given preference in case of a collision. For example, if the same entry is seen on two different interfaces, the value in the `prlvl` column, determines which entry is retained.
Network Layer Address	The IP address of the host from which a packet is received.
Link Layer Address	The MAC address of the host.
Mode	Displays one of the following values: "invalid", "unsupp", "access", "trunk", "vpc", "svi", "virtual", "pseudowire", "unkn", "bdi", "pseudoport".
vlan(prim)	The host's VLAN ID
prlvl	A value between 1 and 100 is displayed, with 1 having the lowest preference level, and 100 having the highest preference level. See `Preflevel flags` above to know what the value displayed here means.
age	The total age of the entry in seconds (s) or minutes (mn) since the the last time the entry was refreshed. When it is refreshed (sign-of-life from the host), this value is reset.
state	The current state of an entry, which can be one of the stable or transitional states. Stable state values are: REACHABLE, DOWN, and STALE, Transitional states values are: VERIFY, INCOMPLETE, and TENTATIVE.

Field	Description
Time left	Displays the amount of time left until the next action in the current state.
In Crimson	A *yes* or *no* value which indicates if the entry has been added to another database. The information is then used by other applications, like Cisco DNA Center. Typically, all the entries that are in a binding table are also added to this database. This is used by the technical support team, for troubleshooting and to diagnose a problem.
Client ID	This field is applicable only to virtual machines (VMs) in Cisco Software-Defined Access (SDA) deployments. It refers to the actual MAC address of a VM in a bridged networking mode, where the hosting device is a wireless client with a non-promiscuous network interface (NIC).
Session ID	This field is applicable only to VMs in SDA deployments. It refers to an access session ID for a VM in a bridged networking mode. Each Session ID is associated with a Client ID. SISF maintains this association and transfers it along as the VM roams or moves across fabric edges in an SDA setup.
Policy (feature)	Displays the name of the policy applied to the interface or VLAN. The "(feature)" displayed is always "Device-tracking", because only SISF-based device-tracking supports the creation of binding entries.

show device-tracking events

To display SISF binding table-related events, enter the **show device-tracking events** command in privileged EXEC mode. The types of events that are displayed includes the creation of binding table entries and all updates to an entry. Updates may be state changes, or, changes in the MAC, VLAN, or interface information for an entry.

show device-tracking events

Syntax Description

This command has no arguments or keywords.

Command Default

SISF binding table events are displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The output of this command is used by the technical support team, for troubleshooting.

Examples

The following is sample output for the **show device-tracking events** command. It shows you the kind of binding table events that the system logs:

```
Device# show device-tracking events
 [Wed Mar 23 19:08:33.000] SSID 0 FSM Feature Table running for event ACTIVE_REGISTER in
state CREATING
 [Wed Mar 23 19:08:33.000] SSID 0 Transition from CREATING to READY upon event ACTIVE_REGISTER

 [Wed Mar 23 19:08:33.000] SSID 1 FSM Feature Table running for event ACTIVE_REGISTER in
state CREATING
 [Wed Mar 23 19:08:33.000] SSID 1 Transition from CREATING to READY upon event ACTIVE_REGISTER

 [Wed Mar 23 19:09:25.000] SSID 0 FSM sisf_mac_fsm running for event MAC_TENTV in state
MAC-CREATING
 [Wed Mar 23 19:09:25.000] SSID 0 Transition from MAC-CREATING to MAC-TENTATIVE upon event
 MAC_TENTV
 [Wed Mar 23 19:09:25.000] SSID 1 Created Entry origin IPv4 ARP MAC 00a5.bf9c.e051 IPV4
10.0.0.1
 [Wed Mar 23 19:09:25.000] SSID 0 FSM sisf_mac_fsm running for event MAC_VERIFIED in state
 MAC-TENTATIVE
 [Wed Mar 23 19:09:25.000] SSID 0 Transition from MAC-TENTATIVE to MAC-REACHABLE upon event
 MAC_VERIFIED
 [Wed Mar 23 19:09:25.000] SSID 1 FSM Binding table running for event VALIDATE_LLA in state
 CREATING
 [Wed Mar 23 19:09:25.000] SSID 1 FSM Binding table running for event SET_TENTATIVE in state
 CREATING
 [Wed Mar 23 19:09:25.000] SSID 1 Transition from CREATING to TENTATIVE upon event
SET_TENTATIVE
 [Wed Mar 23 19:09:25.000] SSID 1 Entry State changed origin IPv4 ARP MAC 00a5.bf9c.e051
IPV4 10.0.0.1
```

```
 [Wed Mar 23 20:07:27.000] SSID 0 FSM sisf_mac_fsm running for event MAC_DELETE_NOS in state
 MAC-REACHABLE
 [Wed Mar 23 20:07:27.000] SSID 0 Transition from MAC-REACHABLE to MAC-NONE upon event
MAC_DELETE_NOS
 [Wed Mar 23 20:07:27.000] SSID 1 Transition from REACHABLE to NONE upon event DELETE
```

show device-tracking features

To display the device-tracking features that are enabled, enter the **show device-tracking features** command in privileged EXEC mode. The "features" include SISF-based device-tracking, and security features like IPv6 RA Guard, IPv6 DHCP Guard, Layer 2 DHCP Relay, and so on, that use SISF.

show device-tracking features

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Examples

The following is sample output for the **show device-tracking features** command.

```
Device# show device-tracking features
Feature name   priority state
Device-tracking   128   READY
Source guard       32   READY
```

show device-tracking messages

To display a list of device-tracking related activities, enter the **show device-tracking messages** command in privileged EXEC mode.

show device-tracking messages [**detailed** *no_of_messages*]

Syntax Description

detailed *no_of_messages*	Displays a more detailed format of the list of device-tracking messages. Enter a value between 1 and 255, to specify the number of messages that must be displayed in a detailed format.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

The following is sample output for the **show device-tracking messages** command. The summarized and detailed versions of the output are displayed:

```
Device# show device-tracking messages
 [Wed Mar 23 19:09:25.000] VLAN 1, From Te1/0/2 MAC 00a5.bf9c.e051: ARP::REP, 10.0.0.1,
 [Wed Mar 23 20:03:22.000] VLAN 1, From Te1/0/2 MAC 00a5.bf9c.e051: ARP::REP, 10.0.0.1,


Device# show device-tracking messages detailed 255
 [Wed Mar 23 19:09:25.000] VLAN 1, From Te1/0/2 seclvl [guard], MAC 00a5.bf9c.e051: ARP::REP,

 1 addresses advertised:
    IPv6 addr: 10.0.0.1,

 [Wed Mar 23 20:03:22.000] VLAN 1, From Te1/0/2 seclvl [guard], MAC 00a5.bf9c.e051: ARP::REP,

 1 addresses advertised:
    IPv6 addr: 10.0.0.1,
```

show device-tracking policies

To display *all* the device-tracking policies on the device, enter the **show device-tracking policies** command in privileged EXEC mode.

show device-tracking policies [**details** | **interface** *interface_type_no* [**details**] | **vlan** *vlanid*]

Syntax Description

details	Displays information about the policy targets and policy parameters of all device-tracking policies on the device
interface *interface_type_no*	Displays all policies applied to the the specified interface. Enter an interface type and number. Use the question mark (?) online help function to display the types of interfaces on the device.
vlan *vlanid*	Displays all policies applied to the the specified VLAN. The valid value range is from 1 to 4095.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Examples

The following is sample output for the **show device-tracking policies** command with the **details** keyword. It shows that there is only one policy on the device. It shows the target to which the policy is applied and the policy parameters.

```
Device# show device-tracking policies details

Target               Type  Policy               Feature        Target range
Te1/0/1              PORT  sisf-01              Device-tracking vlan all

Device-tracking policy sisf-01 configuration:
  security-level guard
  device-role node
  gleaning from Neighbor Discovery
  gleaning from DHCP6
  gleaning from ARP
  gleaning from DHCP4
  NOT gleaning from protocol unkn
  tracking enable
Policy sisf-01 is applied on the following targets:
Target               Type  Policy               Feature        Target range
Te1/0/1              PORT  sisf-01              Device-tracking vlan all
```

show device-tracking policy

To display information about a particular policy, enter the **show device-tracking policy** command in privileged EXEC mode. Displayed information includes the list of targets to which the policy is applied, and policy parameters.

show device-tracking policy *policy_name*

Syntax Description

policy_name	Enter the name of the policy.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Examples

The following is sample output for the **show device-tracking policy** command. Details of policy `sisf-01` are displayed.

```
Device# show device-tracking policy sisf-01
Device-tracking policy sisf-01 configuration:
  security-level guard
  device-role node
  gleaning from Neighbor Discovery
  gleaning from DHCP6
  gleaning from ARP
  gleaning from DHCP4
  NOT gleaning from protocol unkn
  tracking enable
Policy sisf-01 is applied on the following targets:
Target              Type  Policy              Feature        Target range
Te1/0/1             PORT  sisf-01             Device-tracking vlan all
```

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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
-------------------------------------------
RxStart = 0     RxLogoff = 0    RxResp = 0      RxRespID = 0
RxReq = 0       RxInvalid = 0   RxLenErr = 0
RxTotal = 0

TxStart = 0     TxLogoff = 0    TxResp = 0
TxReq = 0       ReTxReq = 0     ReTxReqFail = 0
TxReqID = 0     ReTxReqID = 0   ReTxReqIDFail = 0
TxTotal = 0
```

show eap pac peer

To display stored Protected Access Credentials (PAC) for Extensible Authentication Protocol (EAP) Flexible Authentication via Secure Tunneling (FAST) peers, use the **show eap pac peer** command in privileged EXEC mode.

show eap pac peer

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

The following is sample output from the **show eap pac peers** command:

```
Device# show eap pac peers

No PACs stored
```

Related Commands

Command	Description
clear eap sessions	Clears EAP session information for the device or for the spe

show ip access-lists

To display the contents of all current IP access lists, use the **show ip access-lists** command in user EXEC or privileged EXEC modes.

show ip access-lists [{ *access-list-number access-list-number-expanded-range access-list-name* | **dynamic** [*dynamic-access-list-name*] | **interface** *name number* [{ **in** | **out** }] }]

Syntax Description

access-list-number	(Optional) Number of the IP access list to display.
access-list-number-expanded-range	(Optional) Expanded range of the IP access list to display.
access-list-name	(Optional) Name of the IP access list to display.
dynamic *dynamic-access-list-name*	(Optional) Displays the specified dynamic IP access lists.
interface *name number*	(Optional) Displays the access list for the specified interface.
in	(Optional) Displays input interface statistics.
out	(Optional) Displays output interface statistics.

Note Statistics for OGACL is not supported

Command Default

All standard and expanded IP access lists are displayed.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The **show ip access-lists** command provides output identical to the **show access-lists** command, except that it is IP-specific and allows you to specify a particular access list.

The output of the **show ip access-lists interface** command does not display dACL or ACL filter IDs. This is because the ACLs are attached to the virtual ports created by multidomain authentication for each authentication session; instead of the physical interface. To display dACL or ACL filter IDs, use the **show ip access-lists** *access-list-name* command. The *access-list-name* should be taken from the **show access-session interface** *interface-name* **detail** command output. The *access-list-name* is case sensitive.

Examples

The following is a sample output from the **show ip access-lists** command when all access lists are requested:

```
Device# show ip access-lists

Extended IP access list 101
   deny udp any any eq nntp
   permit tcp any any
   permit udp any any eq tftp
   permit icmp any any
   permit udp any any eq domain
Role-based IP access list r1
    10 permit tcp dst eq telnet
    20 permit udp
FQDN IP access list facl
    10 permit ip host 10.1.1.1 host dynamic www.google.com
    20 permit tcp 10.10.0.0 0.255.255.255 eq ftp host dynamic www.cisco.com log
    30 permit udp host dynamic www.youtube.com any
    40 permit ip 10.3.4.0 0.0.0.255 any
Extended Resolved IP access list facl
    200000 permit tcp 10.0.0.0 0.255.255.255 eq ftp host 10.10.10.1 log
    200001 permit tcp 10.0.0.0 0.255.255.255 eq ftp host 10.10.10.2 log
    300000 permit udp host dynamic 10.11.11.11 any
    300001 permit udp host dynamic 10.11.11.12 any
    400000 permit ip 10.3.4.0 0.0.0.255 any
```

The table below describes the significant fields shown in the display.

Table 144: show ip access-lists Field Descriptions

Field	Description
Extended IP access list	Extended IP access-list name/number.
Role-based IP access list	Role-based IP access-list name.
FQDN IP access list	FQDN IP access-list name.
Extended Resolved IP access list	Extended resolved IP access-list name.
deny	Packets to reject.
udp	User Datagram Protocol.
any	Source host or destination host.
eq	Packets on a given port number.
nntp	Network News Transport Protocol.
permit	Packets to forward.
dynamic	Dynamically resolves domain name.
tcp	Transmission Control Protocol.
tftp	Trivial File Transfer Protocol.
icmp	Internet Control Message Protocol.
domain	Domain name service.

The following is a sample output from the **show ip access-lists** command when the name of a specific access list is requested:

```
Device# show ip access-lists Internetfilter

Extended IP access list Internetfilter
   permit tcp any 192.0.2.0 255.255.255.255 eq telnet
   deny tcp any any
   deny udp any 192.0.2.0 255.255.255.255 lt 1024
   deny ip any any log
```

The following is a sample output from the **show ip access-lists** command using the **dynamic** keyword:

```
Device# show ip access-lists dynamic CM_SF#1

Extended IP access list CM_SF#1
    10 permit udp any any eq 5060 (650 matches)
    20 permit tcp any any eq 5060
    30 permit udp any any dscp ef (806184 matches)
```

Related Commands

Command	Description
deny	Sets conditions in a named IP access list or OGACL that will deny packets.
ip access-group	Applies an ACL or OGACL to an interface or a service policy map.
ip access-list	Defines an IP access list or OGACL by name or number.
object-group network	Defines network object groups for use in OGACLs.
object-group service	Defines service object groups for use in OGACLs.
permit	Sets conditions in a named IP access list or OGACL that will permit packets.
show object-group	Displays information about object groups that are configured.
show run interfaces cable	Displays statistics on the cable modem.

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 Fuji 16.9.2	This command was introduced.

Usage Guidelines

In a device stack, all statistics are generated on the stack's active switch. 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 145: DHCP Snooping Statistics

DHCP Snooping Statistic	Description
Packets Processed by DHCP Snooping	Total number of packets handled by DHCP snooping, including forwarded and dropped packets.
Packets Dropped Because IDB not known	Number of errors when the input interface of the packet cannot be determined.
Queue full	Number of errors when an internal queue used to process the packets is full. This might happen if DHCP packets are received at an excessively high rate and rate limiting is not enabled on the ingress ports.
Interface is in errdisabled	Number of times a packet was received on a port that has been marked as error disabled. This might happen if packets are in the processing queue when a port is put into the error-disabled state and those packets are subsequently processed.
Rate limit exceeded	Number of times the rate limit configured on the port was exceeded and the interface was put into the error-disabled state.
Received on untrusted ports	Number of times a DHCP server packet (OFFER, ACK, NAK, or LEASEQUERY) was received on an untrusted port and was dropped.
Nonzero giaddr	Number of times the relay agent address field (giaddr) in the DHCP packet received on an untrusted port was not zero, or the **no ip dhcp snooping information option allow-untrusted** global configuration command is not configured and a packet received on an untrusted port contained option-82 data.
Source mac not equal to chaddr	Number of times the client MAC address field of the DHCP packet (chaddr) does not match the packet source MAC address and the **ip dhcp snooping verify mac-address** global configuration command is configured.
Binding mismatch	Number of times a RELEASE or DECLINE packet was received on a port that is different than the port in the binding for that MAC address-VLAN pair. This indicates someone might be trying to spoof the real client, or it could mean that the client has moved to another port on the 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.
Insertion of opt82 fail	Number of times the option-82 insertion into a packet failed. The insertion might fail if the packet with the option-82 data exceeds the size of a single physical packet on the internet.

DHCP Snooping Statistic	Description
Interface Down	Number of times the packet is a reply to the DHCP relay agent, but the SVI interface for the relay agent is down. This is an unlikely error that occurs if the SVI goes down between sending the client request to the DHCP server and receiving the response.
Unknown output interface	Number of times the output interface for a DHCP reply packet cannot be determined by either option-82 data or a lookup in the MAC address table. The packet is dropped. This can happen if option 82 is not used and the client MAC address has aged out. If IPSG is enabled with the port-security option and option 82 is not enabled, the MAC address of the client is not learned, and the reply packets will be dropped.
Reply output port equal to input port	Number of times the output port for a DHCP reply packet is the same as the input port, causing a possible loop. Indicates a possible network misconfiguration or misuse of trust settings on ports.
Packet denied by platform	Number of times the packet has been denied by a platform-specific registry.

show 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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Use the **show radius server-group** command to display the server groups that you defined by using the **aaa group server radius** command.

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 146: show radius server-group command Field Descriptions

Field	Description
Server group	Name of the server group.
Sharecount	Number of method lists that are sharing this server group. For example, if one method list uses a particular server group, the sharecount would be 1. If two method lists use the same server group, the sharecount would be 2.
sg_unconfigured	Server group has been unconfigured.

Field	Description
Type	The type can be either standard or nonstandard. The type indicates whether the servers in the group accept nonstandard attributes. If all servers within the group are configured with the nonstandard option, the type will be shown as "nonstandard".
Memlocks	An internal reference count for the server-group structure that is in memory. The number represents how many internal data structure packets or transactions are holding references to this server group. Memlocks is used internally for memory management purposes.

show 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

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.
Cisco IOS XE Gibraltar 16.11.1	

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:

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.

- **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**

- **show platform software fed switch** *switch-number* **acl**
- **show platform software fed switch** *switch-number* **acl usage**
- **show platform software fed switch** *switch-number* **acl policy intftype all cam**
- **show platform software fed switch** *switch-number* **acl cam brief**
- **show platform software fed switch** *switch-number* **acl policy intftype all vcu**
- **show platform hardware fed switch** *switch-number* **acl resource usage**
- **show platform hardware fed switch** *switch-number* **fwd-asic resource tcam table acl**
- **show platform hardware fed switch** *switch-number* **fwd-asic resource tcam utilization**
- **show platform software fed switch** *switch-number* **acl counters hardware**
- **show platform software classification switch** *switch-number* **all F0 class-group-manager class-group**
- **show platform software process database forwarding-manager switch** *switch-number* **R0 summary**
- **show platform software process database forwarding-manager switch** *switch-number* **F0 summary**
- **show platform software object-manager switch** *switch-number* **F0 pending-ack-update**
- **show platform software object-manager switch** *switch-number* **F0 pending-issue-update**
- **show platform software object-manager switch** *switch-number* **F0 error-object**
- **show platform software peer forwarding-manager switch** *switch-number* **F0**
- **show platform software access-list switch** *switch-number* **f0 statistics**
- **show platform software access-list switch** *switch-number* **r0 statistics**
- **show platform software trace message fed switch** *switch-number*
- **show platform software trace message forwarding-manager switch** *switch-number* **F0**
- **show platform software trace message forwarding-manager switch R0** *switch-number* **R0**

Examples

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
```

```
 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
 0x0044 (68)/0xffff     0x0043 (67)/0xffff

 TCP Flags: 0x00 ( NOT SET )

 ACTIONS:  Forward L3, Forward L2, Logging Disabled
 ACL Priority: 2 (15 is Highest Priority)

----------------------------------------
TAQ-4 Index-1 (A:0,C:0) Valid StartF-0 StartA-0 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
 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
 0x0043 (67)/0xffff     0x0044 (68)/0xffff

 TCP Flags: 0x00 ( NOT SET )

 ACTIONS:  Forward L3, Forward L2, Logging Disabled
 ACL Priority: 2 (15 is Highest Priority)

----------------------------------------
TAQ-4 Index-2 (A:0,C:0) Valid StartF-0 StartA-0 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
 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
 0x0043 (67)/0xffff     0x0043 (67)/0xffff

 TCP Flags: 0x00 ( NOT SET )

 ACTIONS:  Forward L3, Forward L2, Logging Disabled
 ACL Priority: 2 (15 is Highest Priority)

----------------------------------------
TAQ-4 Index-3 (A:0,C:0) Valid StartF-0 StartA-0 SkipF-0 SkipA-0
Input 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-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

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.
Cisco IOS XE Gibraltar 16.11.1	

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 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**

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:
```

```
  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 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

  Vlan    Intf-ID   Stp-state
  ------------------------------------------------------------------------------
  1       7           Forwarding
  1       9           Forwarding
  1       17          Forwarding
  1       27          Forwarding
  1       28          Forwarding
  1       29          Forwarding
  1       30          Forwarding
  1       31          Forwarding
  1       40          Forwarding
  1       41          Forwarding


Forwarding Manager Vlan Port Information

  Vlan    Intf-ID   Stp-state
  ------------------------------------------------------------------------------
  1       49          Forwarding
  1       51          Forwarding
  1       63          Forwarding
  1       72          Forwarding
  1       73          Forwarding
  1       74          Forwarding
```

```
------------------ show platform software VP R0 summary ------------------


Forwarding Manager Vlan Port Information

  Vlan    Intf-ID   Stp-state
  ------------------------------------------------------------------------------
  1       7           Forwarding
  1       9           Forwarding
  1       17          Forwarding
  1       27          Forwarding
  1       28          Forwarding
  1       29          Forwarding
  1       30          Forwarding
  1       31          Forwarding
  1       40          Forwarding
  1       41          Forwarding


Forwarding Manager Vlan Port Information

  Vlan    Intf-ID   Stp-state
  ------------------------------------------------------------------------------
  1       49          Forwarding
  1       51          Forwarding
  1       63          Forwarding
  1       72          Forwarding
  1       73          Forwarding
  1       74          Forwarding
.
.
.
```

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Examples

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Examples

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The **show vlan group** command displays the existing VLAN groups and lists the VLANs and VLAN ranges that are members of each VLAN group. If you enter the **group-name** keyword, only the members of the specified VLAN group are displayed.

Examples

This example shows how to display the members of a specified VLAN group:

```
Device# show vlan group group-name group2
vlan group group1 :40-45
```

This example shows how to display number of users in each of the VLANs in a group:

```
Device# show vlan group group-name group2 user_count

  VLAN     : Count
--------------------
  40         : 5
  41         : 8
  42         : 12
  43         : 2
  44         : 9
  45         : 0
```

ssci-based-on-sci

To compute the Short Secure Channel Identifier (SSCI) value based on the Secure Channel Identifier (SCI) value, use the **ssci-based-on-sci** command in MKA-policy configuration mode. To disable SSCI computation based on SCI, use the **no** form of this command.

ssci-based-on-sci
no ssci-based-on-sci

Syntax Description

This command has no arguments or keywords.

Command Default

SSCI value computation based on SCI value is disabled.

Command Modes

MKA-policy configuration (config-mka-policy)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.3	This command was introduced.

Usage Guidelines

The higher the SCI value, the lower is the SSCI value.

Examples

The following example shows how to enable the SSCI computation based on SCI:

```
Device> enable
Device# configure terminal
Device(config)# mka policy 2
Device(config-mka-policy)# ssci-based-on-sci
```

Related Commands

Command	Description
mka policy	Configures an MKA policy.
confidentiality-offset	Sets the confidentiality offset for MACsec operations.
delay-protection	Configures MKA to use delay protection in sending MKPDU.
include-icv-indicator	Includes ICV indicator in MKPDU.
key-server	Configures MKA key-server options.
macsec-cipher-suite	Configures cipher suite for deriving SAK.
sak-rekey	Configures the SAK rekey interval.
send-secure-announcements	Configures MKA to send secure announcements in sending MKPDUs.
use-updated-eth-header	Uses the updated Ethernet header for ICV calculation.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

To enable secure address aging for a particular port, set the aging time to a value other than 0 for that port.

To allow limited time access to particular secure addresses, set the aging type as **absolute**. When the aging time lapses, the secure addresses are deleted.

To allow continuous access to a limited number of secure addresses, set the aging type as **inactivity**. This removes the secure address when it become inactive, and other addresses can become secure.

To allow unlimited access to a secure address, configure it as a secure address, and disable aging for the statically configured secure address by using the **no switchport port-security aging static** interface configuration command.

This example sets the aging time as 2 hours for absolute aging for all the secure addresses on the port:

```
Device> 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** [{*mac-address* | **vlan** {*vlan-id* {**access** | **voice**}}}]}
no switchport port-security mac-address {*mac-address* [{**vlan** {*vlan-id* {**access** | **voice**}}}] | **sticky** [{*mac-address* | **vlan** {*vlan-id* {**access** | **voice**}}}]}

Syntax Description

mac-address	A secure MAC address for the interface by entering a 48-bit MAC address. You can add additional secure MAC addresses up to the maximum value configured.
vlan *vlan-id*	(Optional) On a trunk port only, specifies the VLAN ID and the MAC address. If no VLAN ID is specified, the native VLAN is used.
vlan access	(Optional) On an access port only, specifies the VLAN as an access VLAN.
vlan voice	(Optional) On an access port only, specifies the VLAN as a voice VLAN. **Note** The **voice** keyword is available only if voice VLAN is configured on a port and if that port is not the access VLAN.
sticky	Enables the interface for sticky learning. When sticky learning is enabled, the interface adds all secure MAC addresses that are dynamically learned to the running configuration and converts these addresses to sticky secure MAC addresses.
mac-address	(Optional) A MAC address to specify a sticky secure MAC address.

Command Default

No secure MAC addresses are configured.

Sticky learning is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

A secure port has the following limitations:

- A secure port can be an access port or a trunk port; it cannot be a dynamic access port.
- A secure port cannot be a routed port.
- A secure port cannot be a protected port.
- A secure port cannot be a destination port for Switched Port Analyzer (SPAN).
- A secure port cannot belong to a Gigabit or 10-Gigabit EtherChannel port group.

- You cannot configure static secure or sticky secure MAC addresses in the voice VLAN.
- When you enable port security on an interface that is also configured with a voice VLAN, set the maximum allowed secure addresses on the port to two. When the port is connected to a Cisco IP phone, the IP phone requires one MAC address. The Cisco IP phone address is learned on the voice VLAN, but is not learned on the access VLAN. If you connect a single PC to the Cisco IP phone, no additional MAC addresses are required. If you connect more than one PC to the Cisco IP phone, you must configure enough secure addresses to allow one for each PC and one for the Cisco IP phone.
- Voice VLAN is supported only on access ports and not on trunk ports.

Sticky secure MAC addresses have these characteristics:

- When you enable sticky learning on an interface by using the **switchport port-security mac-address sticky** interface configuration command, the interface converts all the dynamic secure MAC addresses, including those that were dynamically learned before sticky learning was enabled, to sticky secure MAC addresses and adds all sticky secure MAC addresses to the running configuration.
- If you disable sticky learning by using the **no switchport port-security mac-address sticky** interface configuration command or the running configuration is removed, the sticky secure MAC addresses remain part of the running configuration but are removed from the address table. The addresses that were removed can be dynamically reconfigured and added to the address table as dynamic addresses.
- When you configure sticky secure MAC addresses by using the **switchport port-security mac-address sticky** *mac-address* interface configuration command, these addresses are added to the address table and the running configuration. If port security is disabled, the sticky secure MAC addresses remain in the running configuration.
- If you save the sticky secure MAC addresses in the configuration file, when the 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.

switchport port-security maximum *value* [**vlan** [{*vlan-list* | [{**access** | **voice**}]}]]
no switchport port-security maximum *value* [**vlan** [{*vlan-list* | [{**access** | **voice**}]}]]

Syntax Description

value	Sets the maximum number of secure MAC addresses for the interface. The default setting is 1.
vlan	(Optional) For trunk ports, sets the maximum number of secure MAC addresses on a VLAN or range of VLANs. If the **vlan** keyword is not entered, the default value is used.
vlan-list	(Optional) Range of VLANs separated by a hyphen or a series of VLANs separated by commas. For nonspecified VLANs, the per-VLAN maximum value is used.
access	(Optional) On an access port only, specifies the VLAN as an access VLAN.
voice	(Optional) On an access port only, specifies the VLAN as a voice VLAN. **Note** The **voice** keyword is available only if voice VLAN is configured on a port and if that port is not the access VLAN.

Command Default

When port security is enabled and no keywords are entered, the default maximum number of secure MAC addresses is 1.

Command Modes

Interface configuration (config-if

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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
```

switchport port-security violation

To configure secure MAC address violation mode or the action to be taken if port security is violated, use the **switchport port-security violation** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

switchport port-security violation {**protect** | **restrict** | **shutdown** | **shutdown vlan**}
no switchport port-security violation {**protect** | **restrict** | **shutdown** | **shutdown vlan**}

Syntax Description

protect	Sets the security violation protect mode.
restrict	Sets the security violation restrict mode.
shutdown	Sets the security violation shutdown mode.
shutdown vlan	Sets the security violation mode to per-VLAN shutdown.

Command Default

The default violation mode is **shutdown**.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

In the security violation protect mode, when the number of port secure MAC addresses reaches the maximum limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses to drop below the maximum value or increase the number of maximum allowable addresses. You are not notified that a security violation has occurred.

Note We do not recommend configuring the protect mode on a trunk port. The protect mode disables learning when any VLAN reaches its maximum limit, even if the port has not reached its maximum limit.

In the security violation restrict mode, when the number of secure MAC addresses reaches the limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses or increase the number of maximum allowable addresses. An SNMP trap is sent, a syslog message is logged, and the violation counter increments.

In the security violation shutdown mode, the interface is error-disabled when a violation occurs and the port LED turns off. An SNMP trap is sent, a syslog message is logged, and the violation counter increments. When a secure port is in the error-disabled state, you can bring it out of this state by entering the **errdisable recovery cause psecure-violation** global configuration command, or you can manually re-enable it by entering the **shutdown** and **no shutdown** interface configuration commands.

When the security violation mode is set to per-VLAN shutdown, only the VLAN on which the violation occurred is error-disabled.

A secure port has the following limitations:

- A secure port can be an access port or a trunk port; 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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The **tacacs server** command configures the TACACS server using the *name* argument and enters TACACS+ server configuration mode. The configuration is applied once you have finished configuration and exited TACACS+ server configuration mode.

Examples

The following example shows how to configure the TACACS server using the name server1 and enter TACACS+ server configuration mode to perform further configuration:

```
Device> enable
Device# configure terminal
Device(config)# tacacs server server1
Device(config-server-tacacs)# end
```

Related Commands

Command	Description
address ipv6 (TACACS+)	Configures the IPv6 address of the TACACS+ server.
key (TACACS+)	Configures the per-server encryption key on the TACACS+ server.
port (TACACS+)	Specifies the TCP port to be used for TACACS+ connections.
send-nat-address (TACACS+)	Sends a client's post-NAT address to the TACACS+ server.
single-connection (TACACS+)	Enables all TACACS packets to be sent to the same server using a single TCP connection.
timeout(TACACS+)	Configures the time to wait for a reply from the specified TACACS server.

tracking (IPv6 snooping)

To override the default tracking policy on a port, use the **tracking** command in IPv6 snooping policy configuration mode.

tracking {**enable** [**reachable-lifetime** {*value* | **infinite**}] | **disable** [**stale-lifetime** {*value* | **infinite**}

Syntax Description

enable	Enables tracking.
reachable-lifetime	(Optional) Specifies the maximum amount of time a reachable entry is considered to be directly or indirectly reachable without proof of reachability. • The **reachable-lifetime** keyword can be used only with the **enable** keyword. • Use of the **reachable-lifetime** keyword overrides the global reachable lifetime configured by the **ipv6 neighbor binding reachable-lifetime** command.
value	Lifetime value, in seconds. The range is from 1 to 86400, and the default is 300.
infinite	Keeps an entry in a reachable or stale state for an infinite amount of time.
disable	Disables tracking.
stale-lifetime	(Optional) Keeps the time entry in a stale state, which overwrites the global stale-lifetime configuration. • The stale lifetime is 86,400 seconds. • The **stale-lifetime** keyword can be used only with the **disable** keyword. • Use of the **stale-lifetime** keyword overrides the global stale lifetime configured by the **ipv6 neighbor binding stale-lifetime** command.

Command Default

The time entry is kept in a reachable state.

Command Modes

IPv6 snooping configuration (config-ipv6-snooping)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The **tracking** command overrides the default tracking policy set by the **ipv6 neighbor tracking** command on the port on which this policy applies. This function is useful on trusted ports where, for example, you may not want to track entries but want an entry to stay in the binding table to prevent it from being stolen.

The **reachable-lifetime** keyword is the maximum time an entry will be considered reachable without proof of reachability, either directly through tracking or indirectly through IPv6 snooping. After the **reachable-lifetime** value is reached, the entry is moved to stale. Use of the **reachable-lifetime** keyword with the tracking command overrides the global reachable lifetime configured by the **ipv6 neighbor binding reachable-lifetime** command.

The **stale-lifetime** keyword is the maximum time an entry is kept in the table before it is deleted or the entry is proven to be reachable, either directly or indirectly. Use of the **reachable-lifetime** keyword with the **tracking** command overrides the global stale lifetime configured by the **ipv6 neighbor binding stale-lifetime** command.

This example shows how to define an IPv6 snooping policy name as policy1and 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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

When the **trusted-port** command is enabled, limited or no verification is performed when messages are received on ports that have this policy. However, to protect against address spoofing, messages are analyzed so that the binding information that they carry can be used to maintain the binding table. Bindings discovered from these ports will be considered more trustworthy than bindings received from ports that are not configured to be trusted.

This example shows how to define an NDP policy name as policy1, 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
```

use-updated-eth-header

To enable interoperability between devices and any port on a device that includes the updated Ethernet header in MACsec Key Agreement Protocol Data Units (MKPDUs) for integrity check value (ICV) calculation, use the **ssci-based-on-sci** command in MKA-policy configuration mode. To disable the updated ethernet header in MKPDUs for ICV calculation, use the **no** form of this command.

use-updated-eth-header
no use-updated-eth-header

Syntax Description

This command has no arguments or keywords.

Command Default

The Ethernet header for ICV calculation is disabled.

Command Modes

MKA-policy configuration (config-mka-policy)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

The updated Ethernet header is non-standard. Enabling this option ensures that an MACsec Key Agreement (MKA) session between the devices can be set up.

Examples

The following example shows how to enable the updated Ethernet header in MKPDUs for ICV calculation:

```
Device> enable
Device# configure terminal
Device(config)# mka policy 2
Device(config-mka-policy)# use-updated-eth-header
```

Related Commands

Command	Description
mka policy	Configures an MKA policy.
confidentiality-offset	Sets the confidentiality offset for MACsec operations.
delay-protection	Configures MKA to use delay protection in sending MKPDU.
include-icv-indicator	Includes ICV indicator in MKPDU.
key-server	Configures MKA key-server options.
macsec-cipher-suite	Configures cipher suite for deriving SAK.
sak-rekey	Configures the SAK rekey interval.
send-secure-announcements	Configures MKA to send secure announcements in sending MKPDUs.
ssci-based-on-sci	Computes SSCI based on the SCI.

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

name	Hostname, server name, user ID, or command name. The *name* argument can be only one word. Blank spaces and quotation marks are not allowed.
aaa attribute list *aaa-list-name*	(Optional) Uses the specified authentication, authorization, and accounting (AAA) method list.
access-class *access-list-number*	(Optional) Specifies an outgoing access list that overrides the access list specified in the **access-class** command that is available in line configuration mode. It is used for the duration of the user's session.
algorithm-type	(Optional) Specifies the algorithm to use for hashing the plaintext secret for the user. • **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.
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

Release	Modifica
Cisco IOS XE Fuji 16.9.2	This com introduce

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

Command	Description
debug ppp negotiation	Displays PPP packets sent during PPP startup, where PPP option
debug serial-interface	Displays information about a serial connection failure.
debug serial-packet	Displays more detailed serial interface debugging information th using the **debug serial interface** command.

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	Modification
Cisco IOS XE Fuji 16.9.2	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.

Examples

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
```

vlan dot1Q tag native

To enable dot1q (IEEE 802.1Q) tagging for a native VLAN on a trunk port, use the **vlan dot1Q tag native** command in global configuration mode.

To disable this function, use the **no** form of this command.

vlan dot1Q tag native
no vlan dot1Q tag native

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced.

Usage Guidelines

Typically, you configure 802.1Q trunks with a native VLAN ID which strips tagging from all packets on that VLAN.

To maintain the tagging on the native VLAN and drop untagged traffic, use the **vlan dot1q tag native** command. The device will tag the traffic received on the native VLAN and admit only 802.1Q-tagged frames, dropping any untagged traffic, including untagged traffic in the native VLAN.

Control traffic continues to be accepted as untagged on the native VLAN on a trunked port, even when the **vlan dot1q tag native** command is enabled.

Note If the **dot1q tag vlan native** command is configured at global level, dot1x reauthentication will fail on trunk ports.

This example shows how to enable dot1q (IEEE 802.1Q) tagging for native VLANs on all trunk ports on a device:

```
Device(config)# vlan dot1q tag native
Device(config)#
```

Related Commands

Command	Description
show vlan dot1q tag native	Displays the status of tagging on the native VLAN.

vlan filter

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	Name of the VLAN map entry.
vlan-list	Specifies which VLANs to apply the map to.
list	The list of one or more VLANs in the form tt, uu-vv, xx, yy-zz, where spaces around commas and dashes are optional. The range is 1 to 4094.
all	Adds the map to all VLANs.

Command Default

There are no VLAN filters.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

To avoid accidentally dropping too many packets and disabling connectivity in the middle of the configuration process, we recommend that you completely define the VLAN access map before applying it to a VLAN.

Examples

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 mac1 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 *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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

If the named VLAN group does not exist, the **vlan group** command creates the group and maps the specified VLAN list to the group. If the named VLAN group exists, the specified VLAN list is mapped to the group.

The **no** form of the **vlan group** command removes the specified VLAN list from the VLAN group. When you remove the last VLAN from the VLAN group, the VLAN group is deleted.

A maximum of 100 VLAN groups can be configured, and a maximum of 4094 VLANs can be mapped to a VLAN group.

Examples

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 XI

Stack Manager and High Availability

• Stack Manager and High Availability Commands, on page 1445

Stack Manager and High Availability Commands

- main-cpu, on page 1446
- mode sso, on page 1447
- policy config-sync prc reload, on page 1448
- redundancy, on page 1449
- redundancy config-sync mismatched-commands, on page 1450
- redundancy force-switchover, on page 1452
- redundancy reload, on page 1453
- reload, on page 1454
- show redundancy, on page 1455
- show redundancy config-sync, on page 1459
- show switch, on page 1461
- show switch stack-mode, on page 1464
- stack-mac persistent timer, on page 1465
- stack-mac update force, on page 1467
- standby console enable, on page 1468
- switch clear stack-mode, on page 1469
- switch switch-number role, on page 1470
- switch stack port, on page 1471
- switch priority, on page 1472
- switch provision, on page 1473
- switch renumber, on page 1475
- switch renumber, on page 1476

main-cpu

To enter the redundancy main configuration submode and enable the standby , use the **main-cpu** command in redundancy configuration mode.

main-cpu

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Redundancy configuration (config-red)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

From the redundancy main configuration submode, use the **standby console enable** command to enable the standby .

This example shows how to enter the redundancy main configuration submode and enable the standby :

```
Device(config)# redundancy
Device(config-red)# main-cpu
Device(config-r-mc)# standby console enable
Device#
```

mode sso

To set the redundancy mode to stateful switchover (SSO), use the **mode sso** command in redundancy configuration mode.

mode sso

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Redundancy configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The **mode sso** command can be entered only from within redundancy configuration mode.

Follow these guidelines when configuring your system to SSO mode:

- You must use identical Cisco IOS images on the 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 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 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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

This example shows how to specify that the standby 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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The redundancy configuration mode is used to enter the main CPU submode, which is used to enable the standby .

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 .

Use the **exit** command to exit redundancy configuration mode.

This example shows how to enter redundancy configuration mode:

```
(config)# redundancy
(config-red)#
```

This example shows how to enter the main CPU submode:

```
(config)# redundancy
(config-red)# main-cpu
(config-r-mc)#
```

Related Commands

Command	Description
show redundancy	Displays redundancy facility information.

redundancy config-sync mismatched-commands

To allow the standby switch to join the stack if a configuration mismatch occurs between the active and standby switches, use the **redundancy config-sync mismatched-commands** command in privileged EXEC mode.

redundancy config-sync {**ignore** | **validate**} **mismatched-commands**

Syntax Description

ignore	Ignores the mismatched command list.
validate	Revalidates the mismatched command list with the modified running-configuration.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

If the command syntax check in the running configuration of the active switch fails while the standby switch is booting, use the **redundancy config-sync mismatched-commands** command to display the Mismatched Command List (MCL) on the active switch and to reboot the standby switch.

The following is a log entry example for mismatched commands:

```
00:06:31: Config Sync: Bulk-sync failure due to Servicing Incompatibility. Please check
full list of mismatched commands via:
show redundancy config-sync failures mcl
00:06:31: Config Sync: Starting lines from MCL file:
interface GigabitEthernet7/7
! <submode> "interface"
- ip address 192.0.2.0 255.255.255.0
! </submode> "interface"
```

To display all mismatched commands, use the **show redundancy config-sync failures mcl** command.

To clean the MCL, follow these steps:

1. Remove all mismatched commands from the running configuration of the active switch.
2. Revalidate the MCL with a modified running configuration by using the **redundancy config-sync validate mismatched-commands** command.
3. Reload the standby switch.

You can ignore the MCL by doing the following:

1. Enter the **redundancy config-sync ignore mismatched-commands** command.
2. Reload the standby switch; the system changes to SSO mode.

Note If you ignore the mismatched commands, the out-of-sync configuration at the active switch and the standby switch still exists.

3. Verify the ignored MCL with the **show redundancy config-sync ignored mcl** command.

If SSO mode cannot be established between the active and standby switches because of an incompatibility in the configuration file, a mismatched command list (MCL) is generated at the active switch and a reload into route processor redundancy (RPR) mode is forced for the standby switch.

This example shows how to revalidate the mismatched command list with the modified configuration:

```
# redundancy config-sync validate mismatched-commands
#
```

redundancy force-switchover

To force a switchover from the active switch to the standby switch, use the **redundancy force-switchover** command in privileged EXEC mode.

redundancy force-switchover

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Use the **redundancy force-switchover** command to manually switch over to the redundant switch. The redundant switch becomes the new active switch that runs the Cisco IOS XE image, and the modules are reset to their default settings. The old active switch reboots with the new image.

If you use the **redundancy force-switchover** command on the active switch, the switchports on the active switch go down.

If you use this command on a switch that is in a partial ring stack, the following warning message appears:

```
Device# redundancy force-switchover

Stack is in Half ring setup; Reloading a switch might cause stack split
This will reload the active unit and force switchover to standby[confirm]
```

This example shows how to manually switch over from the active to the standby supervisor engine:

```
Device# redundancy force-switchover
Device#
```

redundancy reload

To force a reload of one or all of the switches in the stack, use the **redundancy reload** command in privileged EXEC mode.

redundancy reload {**peer** | **shelf**}

Syntax Description

peer	Reloads the peer unit.
shelf	Reboots all switches in the stack.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Before using this command, see the "Performing a Software Upgrade" section of the for additional information.

Use the **redundancy reload shelf** command to reboot all the switches in the stack.

This example shows how to manually reload all switches in the stack:

```
# redundancy reload shelf
#
```

reload

To reload the and to apply a configuration change, use the **reload** command in privileged EXEC mode.

reload [{**/noverify** | **/verify**}] [{*LINE* | **at** | **cancel** | **in**}]

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.

Command Default

Immediately reloads the and puts a configuration change into effect.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

show redundancy

To display redundancy facility information, use the **show redundancy** command in privileged EXEC mode

show redundancy [{**clients** | **config-sync** | **counters** | **history** [{**reload** | **reverse**}] | {**clients** | **counters**} | **states** | **switchover history** [**domain default**]}]

Syntax Description

clients	(Optional) Displays information about the redundancy facility client.
config-sync	(Optional) Displays a configuration synchronization failure or the ignored mismatched command list (MCL).
counters	(Optional) Displays information about the redundancy facility counter.
history	(Optional) Displays a log of past status and related information for the redundancy facility.
history reload	(Optional) Displays a log of past reload information for the redundancy facility.
history reverse	(Optional) Displays a reverse log of past status and related information for the redundancy facility.
clients	Displays all redundancy facility clients in the specified secondary switch.
counters	Displays all counters in the specified standby switch.
states	(Optional) Displays information about the redundancy facility state, such as disabled, initialization, standby or active.
switchover history	(Optional) Displays information about the redundancy facility switchover history.
domain default	(Optional) Displays the default domain as the domain to display switchover history for.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

This example shows how to display information about the redundancy facility:

```
Device# show redundancy

Redundant System Information :
------------------------------
       Available system uptime = 1 hour, 25 minutes
Switchovers system experienced = 0
              Standby failures = 0
        Last switchover reason = not known
```

```
                Hardware Mode = Duplex
    Configured Redundancy Mode = SSO
     Operating Redundancy Mode = SSO
              Maintenance Mode = Disabled
                Communications = Up

Current Processor Information :
-------------------------------
               Active Location = slot 1
        Current Software state = ACTIVE
       Uptime in current state = 1 hour, 25 minutes
                 Image Version = Cisco IOS Software, Catalyst L3 Switch Software
(CAT9K_LITE_IOSXE), Version 16.9.x
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Sat 29-S
        Configuration register = 0x102

Peer Processor Information :
-----------------------------
              Standby Location = slot 3
        Current Software state = STANDBY HOT
       Uptime in current state = 1 hour, 22 minutes
                 Image Version = Cisco IOS Software, Catalyst L3 Switch Software
(CAT9K_LITE_IOSXE), Version 16.9.x
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Sat 29-S
        Configuration register = 0x102

Device#
```

This example shows how to display redundancy facility client information:

```
Device# show redundancy clients

Group ID =     1
     clientID = 29       clientSeq = 60       Redundancy Mode RF
     clientID = 139      clientSeq = 62       IfIndex
     clientID = 25       clientSeq = 71       CHKPT RF
     clientID = 10001    clientSeq = 85       QEMU Platform RF
     clientID = 77       clientSeq = 87       Event Manager
     clientID = 1340     clientSeq = 104      RP Platform RF
     clientID = 1501     clientSeq = 105      CWAN HA
     clientID = 78       clientSeq = 109      TSPTUN HA
     clientID = 305      clientSeq = 110      Multicast ISSU Consolidation RF
     clientID = 304      clientSeq = 111      IP multicast RF Client
     clientID = 22       clientSeq = 112      Network RF Client
     clientID = 88       clientSeq = 113      HSRP
     clientID = 114      clientSeq = 114      GLBP
     clientID = 225      clientSeq = 115      VRRP
     clientID = 4700     clientSeq = 118      COND_DEBUG RF
     clientID = 1341     clientSeq = 119      IOSXE DPIDX
     clientID = 1505     clientSeq = 120      IOSXE SPA TSM
     clientID = 75       clientSeq = 130      Tableid HA
     clientID = 501      clientSeq = 137      LAN-Switch VTP VLAN

<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 = 135884
     tx buffers unavailable = 0
                 buffers rx = 135109
      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

00:00:04 client added: Redundancy Mode RF(29) seq=60
00:00:04 client added: IfIndex(139) seq=62
00:00:04 client added: CHKPT RF(25) seq=71
00:00:04 client added: QEMU Platform RF(10001) seq=85
00:00:04 client added: Event Manager(77) seq=87
00:00:04 client added: RP Platform RF(1340) seq=104
00:00:04 client added: CWAN HA(1501) seq=105
00:00:04 client added: Network RF Client(22) seq=112
00:00:04 client added: IOSXE SPA TSM(1505) seq=120
00:00:04 client added: LAN-Switch VTP VLAN(501) seq=137
00:00:04 client added: XDR RRP RF Client(71) seq=139
00:00:04 client added: CEF RRP RF Client(24) seq=140
00:00:04 client added: MFIB RRP RF Client(306) seq=150
00:00:04 client added: RFS RF(520) seq=163
00:00:04 client added: klib(33014) seq=167
00:00:04 client added: Config Sync RF client(5) seq=168
00:00:04 client added: NGWC FEC Rf client(10007) seq=173
00:00:04 client added: LAN-Switch Port Manager(502) seq=190
00:00:04 client added: Access Tunnel(530) seq=192
00:00:04 client added: Mac address Table Manager(519) seq=193
00:00:04 client added: DHCPC(100) seq=238
00:00:04 client added: DHCPD(101) seq=239
00:00:04 client added: SNMP RF Client(34) seq=251
00:00:04 client added: CWAN APS HA RF Client(1502) seq=252
00:00:04 client added: History RF Client(35) seq=261

<output truncated>
```

This example shows how to display information about the redundancy facility state:

```
Device# show redundancy states

       my state = 13 -ACTIVE
     peer state = 8  -STANDBY HOT
           Mode = Duplex
           Unit = Primary
        Unit ID = 5

Redundancy Mode (Operational) = sso
Redundancy Mode (Configured)  = sso
Redundancy State              = sso
     Maintenance Mode = Disabled
    Manual Swact = enabled
 Communications = Up

   client count = 115
 client_notification_TMR = 30000 milliseconds
           RF debug mask = 0x0

Device#
```

show redundancy config-sync

To display a configuration synchronization failure or the ignored mismatched command list (MCL), if any, use the **show redundancy config-sync** command in EXEC mode.

show redundancy config-sync {**failures** {**bem** | **mcl** | **prc**} | **ignored failures mcl**}

Syntax Description

failures	Displays MCL entries or best effort method (BEM)/Parser Return Code (PRC) failures.
bem	Displays a BEM failed command list, and forces the standby to reboot.
mcl	Displays commands that exist in the switch's running configuration but are not supported by the image on the standby , and forces the standby to reboot.
prc	Displays a PRC failed command list and forces the standby to reboot.
ignored failures mcl	Displays the ignored MCL failures.

Command Default

None

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

When two versions of Cisco IOS images are involved, the command sets supported by two images might differ. If any of those mismatched commands are executed on the active , the standby might not recognize those commands, which causes a configuration mismatch condition. If the syntax check for the command fails on the standby during a bulk synchronization, the command is moved into the MCL and the standby 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 '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 .

Alternatively, you could ignore the MCL by following these steps:

1. Enter the **redundancy config-sync ignore mismatched-commands** command.
2. Reload the standby ; the system transitions to SSO mode.

Note If you ignore the mismatched commands, the out-of-synchronization configuration on the active and the standby 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 maintains the PRC after executing a command. The standby executes the command and sends the PRC back to the active . A PRC failure occurs if these two PRCs do not match. If a PRC error occurs at the standby either during bulk synchronization or line-by-line (LBL) synchronization, the standby is reset. To display all PRC failures, use the **show redundancy config-sync failures prc** command.

To display best effort method (BEM) errors, use the **show redundancy config-sync failures bem** command.

This example shows how to display the BEM failures:

```
Device> show redundancy config-sync failures bem
BEM Failed Command List
-----------------------

 The list is Empty
```

This example shows how to display the MCL failures:

```
Device> show redundancy config-sync failures mcl
Mismatched Command List
-----------------------

The list is Empty
```

This example shows how to display the PRC failures:

```
Device# show redundancy config-sync failures prc
PRC Failed Command List
-----------------------

 The list is Empty
```

show switch

To display information that is related to the stack member or the switch stack, use the **show switch** command in EXEC mode.

show switch [{*stack-member-number* | **detail** | **neighbors** | **stack-ports** [{**summary**}]}]

Syntax Description

stack-member-number	(Optional) Number of the stack member. The range is 1 to 9.
detail	(Optional) Displays detailed information about the stack ring.
neighbors	(Optional) Displays the neighbors of the entire switch stack.
stack-ports	(Optional) Displays port information for the entire switch stack.
summary	(Optional) Displays the stack cable length, the stack link status, and the loopback status.

Command Default

None

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

This command displays these states:

- Initializing—A switch has been just added to the stack and it has not completed the basic initialization to go to the ready state.
- HA Sync in Progress—After the standby is elected, the corresponding switch remains in this state until the synchronization is completed.
- Syncing—A switch that is added to an already existing stack remains in this state until the switch add sequence is complete.
- Ready—The member has completed loading the system- and interface-level configurations and can forward traffic.
- V-Mismatch—A switch in version mismatch mode. Version-mismatch mode is when a switch that joins the stack has a software version that is incompatible with the active switch.
- Provisioned—The state of a preconfigured switch before it becomes an active member of a switch stack. The MAC address and the priority number in the display are always 0 for the provisioned switch.
- Unprovisioned—The state of a switch when the provisioned switch number was unprovisioned using the **no switch** *switch-number* **provision** command.

- Removed—A switch that was present in the stack was removed using the **reload slot** command.
- Sync not started—When multiple switches are added to an existing stack together, the active switch adds them one by one. The switch that is being added is in the Syncing state. The switches that have not been added yet are in the Sync not started state.
- Lic-Mismatch—A switch has a different license level than the active switch.

A typical state transition for a stack member (including an active switch) booting up is Waiting > Initializing > Ready.

A typical state transition for a stack member in version mismatch (VM) mode is Waiting > Ver Mismatch.

You can use the **show switch** command to identify whether the provisioned switch exists in the switch stack. The **show running-config** and the **show startup-config** privileged EXEC commands do not provide this information.

The display also includes stack MAC-persistency wait-time if persistent MAC address is enabled.

Examples

This example shows how to display summary stack information:

This example shows how to display detailed stack information:

This example shows how to display the member 6 summary information:

```
# show switch 6
Switch#  Role      Mac Address     Priority     State
-------------------------------------------------------
 6       Member     0003.e31a.1e00     1         Ready
```

This example shows how to display the neighbor information for a stack:

```
# show switch neighbors
  Switch #    Port A       Port B
  --------    ------       ------
      6        None           8
      8         6            None
```

This example shows how to display stack-port information:

```
# show switch stack-ports
  Switch #    Port A       Port B
  --------    ------       ------
    6          Down          Ok
    8           Ok          Down
```

This example shows the output for the **show switch stack-ports summary** command. The table that follows describes the fields in the display.

```
# show switch stack-ports summary
Switch#/  Stack   Neighbor   Cable    Link   Link   Sync      #         In
 Port#     Port              Length    OK   Active   OK    Changes   Loopback
          Status                                          To LinkOK
--------  ------  --------  --------  ----  ------  ----  ---------  --------
  1/1     Down      2       50 cm     No     NO      No      10         No
  1/2     Ok        3       1 m       Yes    Yes     Yes     0          No
  2/1     Ok        5       3 m       Yes    Yes     Yes     0          No
  2/2     Down      1       50 cm     No     No      No      10         No
  3/1     Ok        1       1 m       Yes    Yes     Yes     0          No
  3/2     Ok        5       1 m       Yes    Yes     Yes     0          No
```

```
5/1     Ok        3       1 m       Yes    Yes     Yes     0          No
5/2     Ok        2       3 m       Yes    Yes     Yes     0          No
```

Table 147: Show switch stack-ports summary Command Output

Field	Description
Switch#/Port#	Member number and its stack port number.
Stack Port Status	Status of the stack port. • Down—A cable is detected, but either no connected neighbor is up, or the stack port is disabled. • OK—A cable is detected, and the connected neighbor is up.
Neighbor	Switch number of the active member at the other end of the stack cable.
Cable Length	Valid lengths are 50 cm, 1 m, or 3 m. If the switch cannot detect the cable length, the value is *no cable*. The cable might not be connected, or the link might be unreliable.
Link OK	Whether the stack cable is connected and functional. There may or may not be a neighbor connected on the other end. The *link partner* is a stack port on a neighbor switch. • No—There is no stack cable connected to this port or the stack cable is not functional. • Yes—There is a functional stack cable connected to this port.
Link Active	Whether a neighbor is connected on the other end of the stack cable. • No—No neighbor is detected on the other end. The port cannot send traffic over this link. • Yes—A neighbor is detected on the other end. The port can send traffic over this link.
Sync OK	Whether the link partner sends valid protocol messages to the stack port. • No—The link partner does not send valid protocol messages to the stack port. • Yes—The link partner sends valid protocol messages to the port.
# Changes to LinkOK	The relative stability of the link. If a large number of changes occur in a short period of time, link flapping can occur.
In Loopback	Whether a stack cable is attached to a stack port on the member. • No— At least one stack port on the member has an attached stack cable. • Yes—None of the stack ports on the member has an attached stack cable.

show switch stack-mode

To display and verify the current stack mode on a device, use the **show switch stack-mode** command in priviledged EXEC mode.

show switch stack-mode

Command Default None

Command Modes priviledged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.1	This command was introduced.

Usage Guidelines The **show switch stack-mode** command displays detailed status of the currently running stack mode. Fields dispalyed for each one of the devices in the stack include: the role of the device, its MAC address, the stack mode after reboot, the current stack mode, and so on.

```
Device# show switch stack-mode
Switch   Role    Mac Address    Version   Mode    Configured   State
------------------------------------------------------------
1       Member 3c5e.c357.c880             1+1'     Active'     Ready
*2      Active 547c.69de.cd00    V05      1+1'     Standby'    Ready
3       Member 547c.6965.cf80    V05      1+1'     Member'     Ready
```

The Mode field indicates the current stack mode

The Configured field refers to the device state expected after a reboot.

Single quotation marks (') indicate that the stack mode has been changed.

stack-mac persistent timer

To enable the persistent MAC address feature, use the **stack-mac persistent timer** command in global configuration mode on the switch stack or on a standalone switch. To disable the persistent MAC address feature, use the **no** form of this command.

stack-mac persistent timer [{**0***time-value*}]
no stack-mac persistent timer

Syntax Description

0	(Optional) Continues using the MAC address of the current stack's active switch after a new stack's active switch takes over.
time-value	(Optional) Time period in minutes before the stack MAC address changes to that of the new active. The range is 1 to 60 minutes.

Command Default

Persistent MAC address is disabled. The MAC address of the stack is always that of the first active switch.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

By default, the stack MAC address will always be the MAC address of the first active switch, even if a new active switch takes over. The same behavior occurs when you enter the **stack-mac persistent timer** command or the **stack-mac persistent timer 0** command.

Note To avoid PAgP flaps, the stack MAC persistent wait timer should be configured as indefinite using the **stack-mac persistent timer 0** .

When you enter the **stack-mac persistent timer** command with a *time-value*, the stack MAC address will change to that of the new active switch after the period of time that you entered whenever a new switch becomes the active switch. If the previous active switch rejoins the stack during that time period, the stack retains its MAC address for as long as the switch that has that MAC address is in the stack.

If the whole stack reloads the MAC address of the active switch is the stack MAC address.

Note If you do not change the stack MAC address, Layer 3 interface flapping does not occur. This also means that a foreign MAC address (a MAC address that does not belong to any of the switches in the stack) could be the stack MAC address. If the switch with this foreign MAC address joins another stack as the active switch, two stacks will have the same stack MAC address. You must use the **stack-mac update force** command to resolve the conflict.

Examples

This example shows how to enable a persistent MAC address:

```
Device(config)# stack-mac persistent timer
```

You can verify your settings by entering the **show running-config** privileged EXEC command. If enabled, **stack-mac persistent timer** is shown in the output.

stack-mac update force

To update the stack MAC address to the MAC address of the active switch, use the **stack-mac update force** command in EXEC mode on the active switch.

stack-mac update force

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

By default, the stack MAC address is not changed to the MAC address of the new active switch during a high availability (HA) failover. Use the **stack-mac update force** command to force the stack MAC address to change to the MAC address of the new active switch.

If the switch with the same MAC address as the stack MAC address is currently a member of the stack, the **stack-mac update force** command has no effect. (It does not change the stack MAC address to the MAC address of the active switch.)

Note If you do not change the stack MAC address, Layer 3 interface flapping does not occur. It also means that a foreign MAC address (a MAC address that does not belong to any of the switches in the stack) could be the stack MAC address. If the switch with this foreign MAC address joins another stack as the active switch, two stacks will have the same stack MAC address. You must use the **stack-mac update force** command to resolve the conflict.

This example shows how to update the stack MAC address to the MAC address of the active switch:

```
> stack-mac update force
>
```

You can verify your settings by entering the **show switch** privileged EXEC command. The stack MAC address includes whether the MAC address is local or foreign.

standby console enable

To enable access to the standby console , use the **standby console enable** command in redundancy main configuration submode. To disable access to the standby console , 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 is disabled.

Command Modes

Redundancy main configuration submode

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

This command is used to collect and review specific data about the standby console. The command is useful primarily for Cisco technical support representatives troubleshooting the .

This example shows how to enter the redundancy main configuration submode and enable access to the standby console :

```
Device(config)# redundancy
Device(config-red)# main-cpu
Device(config-r-mc)# standby console enable
Device(config-r-mc)#
```

switch clear stack-mode

To change the stack mode to N+1 and remove the active and standby assignemnets of the 1:1 mode, use the **switch clear stack-mode** command in priviledged EXEC mode.

switch clear stack-mode

Command Default

None

Command Modes

priviledged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.1	This command was introduced.

Usage Guidelines

Use this command to disable the 1:1 redundancy mode and set the stack to N+1 mode.

```
Device> enable
Device# switch clear stack-mode
WARNING: Clearing the chassis HA configuration will result in the chassis coming up in Stand
 Alone mode after reboot.The HA configuration will remain the same on other chassis. Do you
 wish to continue? [y/n]? [yes]:
```

switch switch-number role

To change the role of the device in the stack to either active or standby, use the **switch** *switch-number* **role** command in priviledged EXEC mode.

switch *switch-number* **role** {**standby** | **active**}

Syntax Description

Syntax Description	
switch-number	Stack member number.
standby	Designates the device as Standby Device for the stack.
active	Designates the device as Active Device for the stack.

Command Default

None

Command Modes

priviledged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.1	This command was introduced.

Usage Guidelines

Use this command to set a device to active or standby role in the stack. The other devices in the stack remain as members of the stack.

Note Changing the role of the device results in redundancy mode being configured to 1:1 mode for the stack. If the configured active or standby device does not boot up, then the stack will not be able to boot.

The following example sets the device number 2 as active device and device number 1 as standby device for the stack.

```
Device> enable
Device# switch 2 role active
WARNING: Changing the switch role may result in redundancy mode being configured to 1+1
mode for this stack. If the configured Active or Standby switch numbers do not boot up,
then the stack will not be able to boot. Do you want to continue?[y/n]? : yes


Device# switch 1 role standby
WARNING: Changing the switch role may result in redundancy mode being configured to 1+1
mode for this stack. If the configured Active or Standby switch numbers do not boot up,
then the stack will not be able to boot. Do you want to continue?[y/n]? : yes
```

switch stack port

To disable or enable the specified stack port on the member, use the **switch** command in privileged EXEC mode on a stack member.

switch *stack-member-number* **stack port** *port-number* {**disable** | **enable**}

Syntax Description

stack-member-number	Current stack member number. The range is 1 to 8.
stack port *port-number*	Specifies the stack port on the member. The range is 1 to 2.
disable	Disables the specified port.
enable	Enables the specified port.

Command Default

The stack port is enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

A stack is in the full-ring state when all members are connected through the stack ports and are in the ready state.

The stack is in the partial-ring state when the following occurs:

- All members are connected through their stack ports but some are not in the ready state.
- Some members are not connected through the stack ports.

Note Be careful when using the **switch** *stack-member-number* **stack port** *port-number* **disable** command. When you disable the stack port, the stack operates at half bandwidth.

If you enter the **switch** *stack-member-number* **stack port** *port-number* **disable** privileged EXEC command and the stack is in the full-ring state, you can disable only one stack port. This message appears:

```
Enabling/disabling a stack port may cause undesired stack changes. Continue?[confirm]
```

If you enter the **switch** *stack-member-number* **stack port** *port-number* **disable** privileged EXEC command and the stack is in the partial-ring state, you cannot disable the port. This message appears:

```
Disabling stack port not allowed with current stack configuration.
```

Examples

This example shows how to disable stack port 2 on member 4:

```
# switch 4 stack port 2 disable
```

switch priority

To change the stack member priority value, use the **switch priority** command in EXEC mode on the active switch.

switch *stack-member-number* **priority** *new-priority-value*

Syntax Description

stack-member-number	Current stack member number. The range is 1 to 8.
new-priority-value	New stack member priority value. The range is 1 to 15.

Command Default

The default priority value is 1.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The new priority value is a factor when a new active switch is elected. When you change the priority value the active switch is not changed immediately.

Examples

This example shows how to change the priority value of stack member 6 to 8:

```
# switch 6 priority 8
Changing the Switch Priority of Switch Number 6 to 8
Do you want to continue?[confirm]
```

switch provision

To supply a configuration to a new switch before it joins the switch stack, use the **switch provision** command in global configuration mode on the active switch. To delete all configuration information that is associated with the removed switch (a stack member that has left the stack), use the **no** form of this command.

switch *stack-member-number* **provision** *type*
no switch *stack-member-number* **provision**

Syntax Description

stack-member-number	Stack member number. The range is 1 to 8.
type	Switch type of the new switch before it joins the stack.

Command Default

The switch is not provisioned.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

For *type*, enter the model number of a supported switch that is listed in the command-line help strings.

To avoid receiving an error message, you must remove the specified switch from the switch stack before using the **no** form of this command to delete a provisioned configuration.

To change the switch type, you must also remove the specified switch from the switch stack. You can change the stack member number of a provisioned switch that is physically present in the switch stack if you do not also change the switch type.

If the switch type of the provisioned switch does not match the switch type in the provisioned configuration on the stack, the switch stack applies the default configuration to the provisioned switch and adds it to the stack. The switch stack displays a message when it applies the default configuration.

Provisioned information appears in the running configuration of the switch stack. When you enter the **copy running-config startup-config** privileged EXEC command, the provisioned configuration is saved in the startup configuration file of the switch stack.

Caution When you use the **switch provision** command, memory is allocated for the provisioned configuration. When a new switch type is configured, the previously allocated memory is not fully released. Therefore, do not use this command more than approximately 200 times, or the switch will run out of memory and unexpected behavior will result.

Examples

This example shows how to provision a switch with a stack member number of 2 for the switch stack. The **show running-config** command output shows the interfaces associated with the provisioned switch.

```
(config)# switch 2 provision WS-xxxx
(config)# end
```

```
# show running-config | include switch 2
!
interface GigabitEthernet2/0/1
!
interface GigabitEthernet2/0/2
!
interface GigabitEthernet2/0/3
<output truncated>
```

You also can enter the **show switch** user EXEC command to display the provisioning status of the switch stack.

This example shows how to delete all configuration information about stack member 5 when the switch is removed from the stack:

```
(config)# no switch 5 provision
```

You can verify that the provisioned switch is added to or removed from the running configuration by entering the **show running-config** privileged EXEC command.

switch renumber

To change the stack member number, use the **switch renumber** command in EXEC mode on the active switch.

switch *current-stack-member-number* **renumber** *new-stack-member-number*

Syntax Description

current-stack-member-number	Current stack member number. The range is 1 to 8.
new-stack-member-number	New stack member number for the stack member. The range is 1 to 8.

Command Default

The default stack member number is 1.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

If another stack member is already using the member number that you just specified, the active switch assigns the lowest available number when you reload the stack member.

Note If you change the number of a stack member, and no configuration is associated with the new stack member number, that stack member loses its current configuration and resets to its default configuration.

Do not use the **switch** *current-stack-member-number* **renumber** *new-stack-member-number* command on a provisioned switch. If you do, the command is rejected.

Use the **reload slot** *current stack member number* privileged EXEC command to reload the stack member and to apply this configuration change.

Examples

This example shows how to change the member number of stack member 6 to 7:

```
# switch 6 renumber 7
WARNING:Changing the switch number may result in a configuration change for that switch.
The interface configuration associated with the old switch number will remain as a provisioned
 configuration.
Do you want to continue?[confirm]
```

switch renumber

To change the stack member number, use the **switch renumber** command in EXEC mode on the active switch.

switch *current-stack-member-number* **renumber** *new-stack-member-number*

Syntax Description

current-stack-member-number	Current stack member number. The range is 1 to 8.
new-stack-member-number	New stack member number for the stack member. The range is 1 to 8.

Command Default

The default stack member number is 1.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

If another stack member is already using the member number that you just specified, the active switch assigns the lowest available number when you reload the stack member.

Note If you change the number of a stack member, and no configuration is associated with the new stack member number, that stack member loses its current configuration and resets to its default configuration.

Do not use the **switch** *current-stack-member-number* **renumber** *new-stack-member-number* command on a provisioned switch. If you do, the command is rejected.

Use the **reload slot** *current stack member number* privileged EXEC command to reload the stack member and to apply this configuration change.

Examples

This example shows how to change the member number of stack member 6 to 7:

```
# switch 6 renumber 7
WARNING:Changing the switch number may result in a configuration change for that switch.
The interface configuration associated with the old switch number will remain as a provisioned
 configuration.
Do you want to continue?[confirm]
```

PART XII

System Management

- System Management Commands, on page 1479
- Tracing, on page 1637

System Management Commands

- arp, on page 1481
- boot, on page 1482
- boot system, on page 1483
- cat, on page 1484
- copy, on page 1485
- copy startup-config tftp:, on page 1486
- copy tftp: startup-config, on page 1487
- debug voice diagnostics mac-address, on page 1488
- debug platform condition feature multicast controlplane, on page 1489
- debug platform condition mac, on page 1491
- debug platform rep, on page 1492
- debug ilpower powerman, on page 1493
- delete, on page 1496
- dir, on page 1497
- exit, on page 1499
- factory-reset, on page 1500
- flash_init, on page 1502
- help, on page 1503
- install, on page 1504
- l2 traceroute, on page 1508
- license boot level, on page 1509
- license smart deregister, on page 1511
- license smart register idtoken, on page 1512
- license smart renew, on page 1513
- location, on page 1514
- location plm calibrating, on page 1517
- mgmt_init, on page 1518
- mkdir, on page 1519
- more, on page 1520
- no debug all, on page 1521
- rename, on page 1522
- request consent-token accept-response shell-access, on page 1523
- request consent-token generate-challenge shell-access, on page 1524

- request consent-token terminate-auth , on page 1525
- request platform software console attach switch, on page 1526
- reset, on page 1528
- rmdir, on page 1529
- sdm prefer, on page 1530
- service private-config-encryption, on page 1531
- set, on page 1532
- show avc client, on page 1535
- show debug, on page 1536
- show env xps, on page 1537
- show flow monitor, on page 1541
- show install, on page 1546
- show license all, on page 1548
- show license status, on page 1550
- show license summary, on page 1552
- show license udi, on page 1553
- show license usage, on page 1554
- show location, on page 1555
- show logging onboard switch uptime, on page 1557
- show mac address-table, on page 1560
- show mac address-table move update, on page 1565
- show parser encrypt file status, on page 1566
- show platform integrity, on page 1567
- show platform software audit, on page 1568
- show platform software fed switch punt cause, on page 1572
- show platform software fed switch punt cpuq, on page 1574
- show platform sudi certificate, on page 1577
- show running-config, on page 1579
- show sdm prefer, on page 1585
- show tech-support license , on page 1587
- show tech-support platform, on page 1589
- show tech-support platform evpn_vxlan, on page 1593
- show tech-support platform fabric, on page 1595
- show tech-support platform igmp_snooping, on page 1599
- show tech-support platform layer3, on page 1602
- show tech-support platform mld_snooping, on page 1610
- show tech-support port, on page 1617
- show version, on page 1620
- system env temperature threshold yellow, on page 1627
- traceroute mac, on page 1628
- traceroute mac ip, on page 1631
- type, on page 1633
- unset, on page 1634
- version, on page 1636

arp

To display the contents of the Address Resolution Protocol (ARP) table, use the **arp** command in boot loader mode.

arp [*ip_address*]

Syntax Description

ip_address	(Optional) Shows the ARP table or the mapping for a specific IP address.

Command Default

No default behavior or values.

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	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 *flag 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 a bootable image. Separate image names with a semicolon.

Command Default

No default behavior or values.

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

When you enter the **boot** command without any arguments, the device attempts to automatically boot the system by using the information in the BOOT environment variable, if any.

If you supply an image name for the *file-url* variable, the **boot** command attempts to boot the specified image.

When you specify boot loader **boot** command options, they are executed immediately and apply only to the current boot loader session.

These settings are not saved for the next boot operation.

Filenames and directory names are case sensitive.

Example

This example shows how to boot the device using the *new-image.bin* image:

```
Device: set BOOT flash:/new-images/new-image.bin
Device: boot
```

After entering this command, you are prompted to start the setup program.

boot system

To specify which system image to load during the next boot cycle, use the **boot system** command in global configuration mode. To remove the startup system image specification, use the **no** form of this command.

boot system {*filesystem: /file-url* | **switch all** *filesystem: /file-url*}
no boot system [{*filesystem: /file-url* | **switch all [***filesystem: /file-url***]**}]

Syntax Description

filesystem:	Specifies a file system. The options are *bootflash:*, *flash:*, *ftp:*, *http:*, *sftp:*, and *tftp:*.
switch all	Sets the system image for all devices in the stack.
/file-url	The URL of the system image to load at system startup.

Command Default

No default behavior or values.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Examples

This example shows how to boot the system image file named cat9k_lite_iosxe.16.09.03.SPA.bin from the bootflash:

```
Device(config)# boot system bootflash:cat9k_lite_iosxe.16.09.03.SPA.bin
```

This example shows how to boots all devices in the stack from a network server with an IP address:

```
Device(config)# boot system switch all tftp://10.11.15.10/cat9k_lite_iosxe.16.09.03.SPA.bin
```

cat

To display the contents of one or more files, use the **cat** command in boot loader mode.

cat *filesystem:/file-url...*

Syntax Description

filesystem:	Specifies a file system.
/file-url	Specifies the path (directory) and name of the files to display. Separate each filename with a space.

Command Default

No default behavior or values.

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Filenames and directory names are case sensitive.

If you specify a list of files, the contents of each file appears sequentially.

Examples

This example shows how to display the contents of an image file:

```
Device: cat flash:image_file_name
version_suffix: universal-122-xx.SEx
version_directory: image_file_name
image_system_type_id: 0x00000002
image_name: image_file_name.bin
ios_image_file_size: 8919552
total_image_file_size: 11592192
image_feature: IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
image_family: family
stacking_number: 1.34
board_ids: 0x00000068 0x00000069 0x0000006a 0x0000006b
info_end:
```

copy

To copy a file from a source to a destination, use the **copy** command in boot loader mode.

copy *filesystem:/source-file-url filesystem:/destination-file-url*

Syntax Description

filesystem:	Alias for a file system. Use **usbflash0:** for USB memory sticks.
/source-file-url	Path (directory) and filename (source) to be copied.
/destination-file-url	Path (directory) and filename of the destination.

Command Default

No default behavior or values.

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Filenames and directory names are case sensitive.

Directory names are limited to 127 characters between the slashes (/); the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

Filenames are limited to 127 characters; the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

If you are copying a file to a new directory, the directory must already exist.

Examples

This example shows how to copy a file at the root:

```
Device: copy usbflash0:test1.text usbflash0:test4.text
File "usbflash0:test1.text" successfully copied to "usbflash0:test4.text"
```

You can verify that the file was copied by entering the **dir** *filesystem:* boot loader command.

copy startup-config tftp:

To copy the configuration settings from a switch to a TFTP server, use the **copy startup-config tftp:** command in Privileged EXEC mode.

copy startup-config tftp: *remote host {ip-address}/{name}*

Syntax Description

remote host {ip-address}/{name}	Host name or IP-address of Remote host.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Release 16.1	This command was introduced.

Usage Guidelines

To copy your current configurations from the switch, run the command **copy startup-config tftp:** and follow the instructions. The configurations are copied onto the TFTP server.

Then, login to another switch and run the command **copy tftp: startup-config** and follow the instructions. The configurations are now copied onto the other switch.

Examples

This example shows how to copy the configuration settings onto a TFTP server:

```
Device: copy startup-config tftp:
Address or name of remote host []?
```

copy tftp: startup-config

To copy the configuration settings from a TFTP server onto a new switch, use the **copy tftp: startup-config** command in Privileged EXEC mode on the new switch.

copy tftp: startup-config *remote host {ip-address}/{name}*

Syntax Description

remote host {ip-address}/{name}	Host name or IP-address of Remote host.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Release 16.1	This command was introduced.

Usage Guidelines

After the configurations are copied, to save your configurations, use **write memory** command and then either reload the switch or run the **copy startup-config running-config** command.

Examples

This example shows how to copy the configuration settings from the TFTP server onto a switch:

```
Device: copy tftp: startup-config
Address or name of remote host []?
```

debug voice diagnostics mac-address

To enable debugging of voice diagnostics for voice clients, use the **debug voice diagnostics mac-address** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug voice diagnostics mac-address *mac-address1* **verbose mac-address** *mac-address2* **verbose**
nodebug voice diagnostics mac-address *mac-address1* **verbose mac-address** *mac-address2* **verbose**

Syntax Description

voice diagnostics	Configures voice debugging for voice clients.
mac-address *mac-address1* **mac-address** *mac-address2*	Specifies MAC addresses of the voice clients.
verbose	Enables verbose mode for voice diagnostics.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

The following is sample output from the **debug voice diagnostics mac-address** command and shows how to enable debugging of voice diagnostics for voice client with MAC address of 00:1f:ca:cf:b6:60:

```
Device# debug voice diagnostics mac-address 00:1f:ca:cf:b6:60
```

debug platform condition feature multicast controlplane

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 controlplane** command in privileged EXEC mode. To disable radioactive tracing, use the **no** form of this command.

debug platform condition feature multicast controlplane {{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 controlplane {{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

igmp-debug	Enables IGMP control radioactive tracing.
pim	Enables Protocol Independent Multicast (PIM) control radioactive tracing.
mld-snooping	Enables MLD snooping control radioactive tracing.
igmp-snooping	Enables IGMP snooping control radioactive tracing.
mac *mac-address*	MAC address of the receiver.
group-ip {*ipv4 address* | *ipv6 address***}**	IPv4 or IPv6 address of the igmp-debug or pim group.
ip {*ipv4 address* | *ipv6 address***}**	IPv4 or IPv6 address of the mld-snooping or igmp-snooping group.
vlan *vlan-id*	VLAN ID. The range is from 1 to 4094.
level	Enables debug severity levels.
debug	Enables debugging level.
error	Enables error debugging.
info	Enables information debugging.
verbose	Enables detailed debugging.
warning	Enables warning debugging.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

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

Command	Description
clear debug platform condition all	Removes the debug conditions applied to a platform.
debug platform condition	Filters debugging output for **debug** commands on the basis of specified conditions.
debug platform condition start	Starts conditional debugging on a system.
debug platform condition stop	Stops conditional debugging on a system.
show platform condition	Displays the currently active debug configuration.

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.

debug 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

mac *mac-address*	Filters output on the basis of the specified MAC address.
access-list *access-list name*	Filters output on the basis of the specified access list.
control-plane	Displays messages about the control plane routines.
egress	Filters output on the basis of outgoing packets.
ingress	Filters output on the basis of incoming packets.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

The following example shows how to filter debugging output on the basis of a MAC address:

```
Device# debug platform condition mac bc16.6509.3314 ingress
```

Related Commands

Command	Description
show platform condition	Displays the currently active debug configuration.
debug platform condition	Filters debugging output for **debug** commands on the basis of specified conditions.
debug platform condition start	Starts conditional debugging on a system.
debug platform condition stop	Stops conditional debugging on a system.
clear debug platform condition all	Removes the debug conditions applied to a platform.

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

all	Enables all REP debugging functions.
error	Enables REP error debugging.
event	Enables REP event debugging.
packet	Enables REP packet debugging.
verbose	Enables REP verbose debugging.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

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

Command	Description
show platform condition	Displays the currently active debug configuration.
debug platform condition	Filters debugging output for **debug** commands on the basis of specified conditions.
debug platform condition start	Starts conditional debugging on a system.
debug platform condition stop	Stops conditional debugging on a system.
clear debug platform condition all	Removes the debug conditions applied to a platform.

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

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

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 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[] = 2640 0 0 0 0
Mar 8 16:35:17.801:
Mar 8 16:35:17.801: ILP:: Sending icutoffcurrent msgto slot:1 port:48
Mar 8 16:35:17.802: Ilpowerinterface (Gi1/0/48) power negotiation:
consumption = 2640, alloc_power= 2640
Mar 8 16:35:17.802: Ilpowerinterface (Gi1/0/48) setting ICUT_OFF threshold
 to 2640.
Mar 8 16:35:17.802: ILP:: Sending icutoffcurrent msgto slot:1 port:48
Mar 8 16:35:17.802: ILP:: Sending icutoffcurrent msgto slot:1 port:48
Mar 8 16:35:17.803: ILP:: Sending icutoffcurrent msgto slot:1 port:48
Mar 8 16:35:17.803: ILP:: Sending icutoffcurrent msgto slot:1 port:48
Mar 8 16:35:17.803: ILP:: Sending icutoffcurrent msgto 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 pdlinkdownGi1/0/48
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 msgto slot:1 port:48
Mar 8 16:35:18.116: ilpower_notify_lldp_power_via_mdi_tlvGi1/0/48 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:
```

```
(curr/prev) PSE Allocation: 13000/0
(curr/prev) PD Request : 13000/0
(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/prevPower Pair) : Signal/
(curr/prev) PSE PwrSource : Primary/Unknown
```

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: ILP:: Sending icutoffcurrent msgto slot:1 port:48
Mar 8 16:35:17.802: Ilpowerinterface (Gi1/0/48) power negotiation:
consumption = 2640, alloc_power= 2640
Mar 8 16:35:17.802: Ilpowerinterface (Gi1/0/48) setting ICUT_OFF threshold
 to 2640.
Mar 8 16:35:17.802: ILP:: Sending icutoffcurrent msgto slot:1 port:48
Mar 8 16:35:17.802: ILP:: Sending icutoffcurrent msgto slot:1 port:48
Mar 8 16:35:17.803: ILP:: Sending icutoffcurrent msgto slot:1 port:48
Mar 8 16:35:17.803: ILP:: Sending icutoffcurrent msgto slot:1 port:48
Mar 8 16:35:17.803: ILP:: Sending icutoffcurrent msgto 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 pdlinkdownGi1/0/48
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 msgto slot:1 port:48
Mar 8 16:35:18.116: ilpower_notify_lldp_power_via_mdi_tlvGi1/0/48 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:
(curr/prev) PSE Allocation (mW): 13000/0
<------------------------- mW unit added
(curr/prev) PD Request (mW) : 13000/0
<------------------------- mW unit added
```

```
(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/prevPower 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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Filenames and directory names are case sensitive.

The device prompts you for confirmation before deleting each file.

Examples

This example shows how to delete two files:

```
Device: delete usbflash0:test2.text usbflash0:test5.text
Are you sure you want to delete "usbflash0:test2.text" (y/n)?y
File "usbflash0:test2.text" deleted
Are you sure you want to delete "usbflash0:test5.text" (y/n)?y
File "usbflash0:test2.text" deleted
```

You can verify that the files were deleted by entering the **dir usbflash0:** boot loader command.

dir

To display the list of files and directories on the specified file system, use the **dir** command in boot loader mode.

dir *filesystem:/file-url*

Syntax Description

filesystem:	Alias for a file system. Use **flash:** for the system board flash device; use **usbflash0:** for USB memory sticks.
/file-url	(Optional) Path (directory) and directory name that contain the contents you want to display. Separate each directory name with a space.

Command Default

No default behavior or values.

Command Modes

Boot Loader

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Directory names are case sensitive.

Examples

This example shows how to display the files in flash memory:

```
Device: dir flash:
Directory of flash:/
    2  -rwx         561   Mar 01 2013 00:48:15  express_setup.debug
    3  -rwx     2160256   Mar 01 2013 04:18:48  c2960x-dmon-mz-150-2r.EX
    4  -rwx        1048   Mar 01 2013 00:01:39  multiple-fs
    6  drwx         512   Mar 01 2013 23:11:42  c2960x-universalk9-mz.150-2.EX
  645 drwx         512   Mar 01 2013 00:01:11  dc_profile_dir
  647 -rwx        4316   Mar 01 2013 01:14:05  config.text
  648 -rwx           5   Mar 01 2013 00:01:39  private-config.text

  96453632 bytes available (25732096 bytes used)
```

Table 148: dir Field Descriptions

Field	Description
2	Index number of the file.
-rwx	File permission, which can be any or all of the following: • d—directory • r—readable • w—writable • x—executable

Field	Description
1644045	Size of the file.
<date>	Last modification date.
env_vars	Filename.

exit

To return to the previous mode or exit from the CLI EXEC mode, use the **exit** command.

exit

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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.

Note The erasure is consistent with the clear method, as described in NIST SP 800-88 Rev. 1.

factory-reset {**all [secure 3-pass]** | **boot-vars** | **config**}

Syntax Description

all	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.
secure 3-pass	Erases all the content from the device with 3-pass overwrite. • Pass 1: Overwrites all addressable locations with binary zeroes. • Pass 2: Overwrites all addressable locations with binary ones. • Pass 3: Overwrites all addressable locations with a random bit pattern.
boot-vars	Erases only the user-added boot variables.
config	Erases only the startup configurations.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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]
```

flash_init

To initialize the flash: file system, use the **flash_init** command in boot loader mode.

flash_init

Syntax Description

This command has no arguments or keywords.

Command Default

The flash: file system is automatically initialized during normal system operation.

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

During the normal boot process, the flash: file system is automatically initialized.

Use this command to manually initialize the flash: file system. For example, you use this command during the recovery procedure for a lost or forgotten password.

help

To display the available commands, use the **help** command in boot loader mode.

help

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Example

This example shows how to display a list of available boot loader commands:

```
Device:help
? -- Present list of available commands
arp -- Show arp table or arp-resolve an address
boot -- Load and boot an executable image
cat -- Concatenate (type) file(s)
copy -- Copy a file
delete -- Delete file(s)
dir -- List files in directories
emergency-install -- Initiate Disaster Recovery
...
...
...
unset -- Unset one or more environment variables
version -- Display boot loader version
```

install

To install Software Maintenance Upgrade (SMU) packages, use the **install** command in privileged EXEC mode.

install {**abort** | **activate** | **file** {**bootflash:** | **flash:** | **harddisk:** | **webui:**} [{**auto-abort-timer timer** *timer* **prompt-level** {**all** | **none**}}] | **add file** {**bootflash:** | **flash:** | **ftp:** | **harddisk:** | **http:** | **https:** | **rcp:** | **scp:** | **tftp:** | **webui:**} [{**activate** [{**auto-abort-timer** *timer* **prompt-level** {**all** | **none**}**commit**}]}] | **commit** | **auto-abort-timer stop** | **deactivate file** {**bootflash:** | **flash:** | **harddisk:** | **webui:**} | **label** *id*{**description** *description* | **label-name** *name*} | **remove** {**file** {**bootflash:** | **flash:** | **harddisk:** | **webui:**} | **inactive** } | **rollback to** {**base** | **committed** | **id** {*install-ID* } | **label** {*label-name*}}}

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 *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.
{ **bootflash:** | **flash:** |**ftp:** |**harddisk:** |**http:** |**https:** | **rcp:** | **scp:** | **tftp:** |**webui:**}	Specifies the package to be added.

commit	Makes SMU changes persistent over reloads. You can perform a commit after activating a package while the system is up, or after the first reload. If a package is activated, but not committed, it remains active after the first reload, but not after the second reload.
auto-abort-timer stop	Stops the auto-abort timer.
deactivate	Deactivates an installed package. **Note** Deactivating a package also updates the package status and might trigger a process restart or reload.
label *id*	Specifies the ID of the install point to label.
description	Adds a description to the specified install point.
label-name *name*	Adds a label name to the specified install point.
remove	Removes the installed packages. The **remove** keyword can only be used on packages that are currently inactive.
inactive	Removes all the inactive packages from the device.
rollback	Rolls back the data model interface (DMI) package SMU to the base version, the last committed version, or a known commit ID.
to base	Returns to the base image.
committed	Returns to the installation state when the last commit operation was performed.
id *install-ID*	Returns to the specific install point ID. Valid values are from 1 to 4294967295.

Command Default

Packages are not installed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.1	This command was introduced.

Usage Guidelines

An SMU is a package that can be installed on a system to provide a patch fix or security resolution to a released image. This package 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....

Executing pre scripts done.
--- 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
/flash/cat9k_iosxe.BLD_SMU_20180302_085005_TWIG_LATEST_20180306_013805.3.SSA.smu.bin Mon
Mar  5 21:49:00 PST 2018
```

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 sripts 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
/flash/cat9k_iosxe.BLD_SMU_20180302_085005_TWIG_LATEST_20180306_013805.3.SSA.smu.bin Mon
Mar  5 21:49:34 PST 2018
```

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 sripts 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
```

Related Commands

Command	Description
show install	Displays information about the install packages.

l2 traceroute

To enable the Layer 2 traceroute server, use the **l2 traceroute** command in global configuration mode. Use the **no** form of this command to disable the Layer 2 traceroute server.

l2 traceroute
no l2 traceroute

Syntax Description

This command has no arguments or keywords.

Command Modes

Global configuration (config#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	The command was introduced.

Usage Guidelines

Layer 2 traceroute is enabled by default and opens a listening socket on User Datagram Protocol (UDP) port 2228. To close the UDP port 2228 and disable Layer 2 traceroute, use the **no l2 traceroute** command in global configuration mode.

The following example shows how to configure Layer 2 traceroute using the **l2 traceroute** command.

```
Device# configure terminal
Device(config)# l2 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

Release	Modification
Cisco IOS XE Fuji 16.9.1	This command was introduced.

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.

Examples

The following example shows how to activate the *network-essentals* license on a switch at the next reload:

```
Device(config)# license boot level network-essentals
```

license smart deregister

To cancel device registration from Cisco Smart Software Manager (CSSM), use the **license smart deregister** command in privileged EXEC mode.

license smart deregister

Syntax Description

This command has no arguments or keywords.

Command Default

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.1	This command was introduced.

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

Command	Description
license smart register idtoken	Registers a device in CSSM.
show license all	Displays entitlements information.
show license status	Displays compliance status of a license.
show license summary	Displays summary of all active licenses.
show license usage	Displays license usage information

license smart register idtoken

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

Release	Modification
Cisco IOS XE Fuji 16.9.1	This command was introduced.

Example

This example shows how to register a device on CSSM:

```
Device# license smart register idtoken
$Tl4UytrNXBzbEs1ck8veUtWaG5abnZJOFdDa1FwbVRa%0AblRMbz0%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

Command	Description
license smart deregister	Cancels the device registration from CSSM.
show license all	Displays entitlements information.
show license status	Displays compliance status of a license.
show license summary	Displays summary of all active licenses.
show license usage	Displays license usage information

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

auth	Renews your authorization.
id	Renews your ID.

Command Default

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.1	This command was introduced.

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

Command	Description
show license all	Displays entitlements information.
show license status	Displays compliance status of a license.
show license usage	Displays license usage information

location

To configure location information for an endpoint, use the **location** command in global configuration mode. To remove the location information, use the **no** form of this command.

location {**admin-tag** *string* | **civic-location identifier** {**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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

After entering the **location civic-location identifier** global configuration command, you enter civic location configuration mode. After entering the **location geo-location identifier** global configuration command, you enter geo location configuration mode.

The civic-location identifier must not exceed 250 bytes.

The host identifier configures the host civic or geo-spatial location. If the identifier is not a host, the identifier only defines a civic location or geo-spatial template that can be referenced on the interface.

The **host** keyword defines the device location. The civic location options available for configuration using the **identifier** and the **host** keyword are the same. You can specify the following civic location options in civic location configuration mode:

- **additional-code**—Sets an additional civic location code.
- **additional-location-information**—Sets additional civic location information.
- **branch-road-name**—Sets the branch road name.
- **building**—Sets building information.
- **city**—Sets the city name.
- **country**—Sets the two-letter ISO 3166 country code.
- **county**—Sets the county name.
- **default**—Sets a command to its defaults.
- **division**—Sets the city division name.
- **exit**—Exits from the civic location configuration mode.
- **floor**—Sets the floor number.
- **landmark**—Sets landmark information.
- **leading-street-dir**—Sets the leading street direction.
- **name**—Sets the resident name.
- **neighborhood**—Sets neighborhood information.
- **no**—Negates the specified civic location data and sets the default value.
- **number**—Sets the street number.
- **post-office-box**—Sets the post office box.
- **postal-code**—Sets the postal code.
- **postal-community-name**—Sets the postal community name.
- **primary-road-name**—Sets the primary road name.
- **road-section**—Sets the road section.
- **room**—Sets room information.
- **seat**—Sets seat information.
- **state**—Sets the state name.
- **street-group**—Sets the street group.
- **street-name-postmodifier**—Sets the street name postmodifier.
- **street-name-premodifier**—Sets the street name premodifier.
- **street-number-suffix**—Sets the street number suffix.
- **street-suffix**—Sets the street suffix.
- **sub-branch-road-name**—Sets the sub-branch road name.
- **trailing-street-suffix**—Sets the trailing street suffix.
- **type-of-place**—Sets the type of place.
- **unit**—Sets the unit.

You can specify the following geo-spatial location information in geo-location configuration mode:

- **altitude**—Sets altitude information in units of floor, meters, or feet.
- **latitude**—Sets latitude information in degrees, minutes, and seconds. The range is from -90 degrees to 90 degrees. Positive numbers indicate locations north of the equator.

- **longitude**—Sets longitude information in degrees, minutes, and seconds. The range is from -180 degrees to 180 degrees. Positive numbers indicate locations east of the prime meridian.
- **resolution**—Sets the resolution for latitude and longitude. If the resolution value is not specified, default value of 10 meters is applied to latitude and longitude resolution parameters. For latitude and longitude, the resolution unit is measured in meters. The resolution value can also be a fraction.
- **default**—Sets the geographical location to its default attribute.
- **exit**—Exits from geographical location configuration mode.
- **no**—Negates the specified geographical parameters and sets the default value.

Use the **no lldp med-tlv-select location information** interface configuration command to disable the location TLV. The location TLV is enabled by default.

This example shows how to configure civic location information on the switch:

```
Device(config)# location civic-location identifier 1
Device(config-civic)# number 3550
Device(config-civic)# primary-road-name "Cisco Way"
Device(config-civic)# city "San Jose"
Device(config-civic)# state CA
Device(config-civic)# building 19
Device(config-civic)# room C6
Device(config-civic)# county "Santa Clara"
Device(config-civic)# country US
Device(config-civic)# end
```

You can verify your settings by entering the **show location civic-location** privileged EXEC command.

This example shows how to configure the emergency location information on the switch:

```
Device(config)# location elin-location 14085553881 identifier 1
```

You can verify your settings by entering the **show location elin** privileged EXEC command.

The example shows how to configure geo-spatial location information on the switch:

```
Device(config)# location geo-location identifier host
Device(config-geo)# latitude 12.34
Device(config-geo)# longitude 37.23
Device(config-geo)# altitude 5 floor
Device(config-geo)# resolution 12.34
```

You can use the **show location geo-location identifier** command to display the configured geo-spatial location details.

location plm calibrating

To configure path loss measurement (CCX S60) request for calibrating clients, use the **location plm calibrating** command in global configuration mode.

location plm calibrating {**multiband** | **uniband**}

Syntax Description

multiband	Specifies the path loss measurement request for calibrating clients on the associated 802.11a or 802.11b/g radio.
uniband	Specifies the path loss measurement request for calibrating clients on the associated 802.11a/b/g radio.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The uniband is useful for single radio clients (even if the radio is a dual band and can operate in the 2.4-GHz and the 5-GHz bands). The multiband is useful for multiple radio clients.

This example shows how to configure the path loss measurement request for calibrating clients on the associated 802.11a/b/g radio:

```
Device# configure terminal
Device(config)# location plm calibrating uniband
Device(config)# end
```

mgmt_init

To initialize the Ethernet management port, use the **mgmt_init** command in boot loader mode.

mgmt_init

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Use the **mgmt_init** command only during debugging of the Ethernet management port.

Examples

This example shows how to initialize the Ethernet management port:

```
Device: mgmt_init
```

mkdir

To create one or more directories on the specified file system, use the **mkdir** command in boot loader mode.

mkdir *filesystem:/directory-url...*

Syntax Description

filesystem:	Alias for a file system. Use **usbflash0:** for USB memory sticks.
/directory-url...	Name of the directories to create. Separate each directory name with a space.

Command Default

No default behavior or values.

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Directory names are case sensitive.

Directory names are limited to 127 characters between the slashes (/); the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

Example

This example shows how to make a directory called Saved_Configs:

```
Device: mkdir usbflash0:Saved_Configs
Directory "usbflash0:Saved_Configs" created
```

more

To display the contents of one or more files, use the **more** command in boot loader mode.

more *filesystem:/file-url...*

Syntax Description

filesystem:	Alias for a file system. Use **flash:** for the system board flash device.
/file-url...	Path (directory) and name of the files to display. Separate each filename with a space.

Command Default

No default behavior or values.

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Filenames and directory names are case sensitive.

If you specify a list of files, the contents of each file appears sequentially.

Examples

This example shows how to display the contents of a file:

```
Device: more flash:image_file_name
version_suffix: universal-122-xx.SEx
version_directory: image_file_name
image_system_type_id: 0x00000002
image_name: image_file_name.bin
ios_image_file_size: 8919552
total_image_file_size: 11592192
image_feature: IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
image_family: family
stacking_number: 1.34
board_ids: 0x00000068 0x00000069 0x0000006a 0x0000006b
info_end:
```

no debug all

To disable debugging on a switch, use the **no debug all** command in Privileged EXEC mode.

no debug all

Command Default No default behavior or values.

Command Modes Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Release 16.1	This command was introduced.

Examples This example shows how to disable debugging on a switch.

```
Device: no debug all
All possible debugging has been turned off.
```

rename

To rename a file, use the **rename** command in boot loader mode.

rename *filesystem:/source-file-url filesystem:/destination-file-url*

Syntax Description

filesystem:	Alias for a file system. Use **usbflash0:** for USB memory sticks.
/source-file-url	Original path (directory) and filename.
/destination-file-url	New path (directory) and filename.

Command Default

No default behavior or values.

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Filenames and directory names are case sensitive.

Directory names are limited to 127 characters between the slashes (/); the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

Filenames are limited to 127 characters; the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

Examples

This example shows a file named *config.text* being renamed to *config1.text*:

```
Device: rename usbflash0:config.text usbflash0:config1.text
```

You can verify that the file was renamed by entering the **dir** *filesystem:* boot loader command.

request 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

Syntax	Description
response-string	Specifies the character string representing the response.

Command Modes

Privileged EXEC mode (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

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
[redacted]
% 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

Syntax	Description
auth-timeout *time-validity-slot*	Specifies the time slot in minutes for which shell-access is requested.

Command Modes

Privileged EXEC mode (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

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
zSSdrAAAAQEBAAQAAAABAgAEAAAAAAMACH86csUhmDl0BAAQ0Fvd7CxqRYUeoD7B4AwW7QUABAAAAG8GAAhDVEFfREVNTwAGENUQV9ERU1PX0NUQV9ISUdOSU5HX0tFWQgAC0M5ODAwLUNMLUs5CQALOVpQUEVMSE5KRkI=
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

Privileged EXEC mode (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

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#
*Mar 13 01:45:39.197: %CTOKEN-6-AUTH_UPDATE: Consent Token Update (terminate authentication:
 Shell access 0).
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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

To start a session on the standby switch, you must first enable it in the configuration.

Examples

This example shows how to session to the standby switch:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# redundancy
Device(config-red)# main-cpu
Device(config-r-mc)# standby console enable
Device(config-r-mc)# end
```

```
Device# request platform software console attach switch standby R0
#
# Connecting to the IOS console on the route-processor in slot 0.
# Enter Control-C to exit.
#
Device-stby> enable
Device-stby#
```

reset

To perform a hard reset on the system, use the **reset** command in boot loader mode. A hard reset is similar to power-cycling the device; it clears the processor, registers, and memory.

reset

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Examples

This example shows how to reset the system:

```
Device: reset
Are you sure you want to reset the system (y/n)? y
System resetting...
```

rmdir

To remove one or more empty directories from the specified file system, use the **rmdir** command in boot loader mode.

rmdir *filesystem:/directory-url...*

Syntax Description

filesystem:	Alias for a file system. Use **usbflash0:** for USB memory sticks.
/directory-url...	Path (directory) and name of the empty directories to remove. Separate each directory name with a space.

Command Default

No default behavior or values.

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Directory names are case sensitive and limited to 45 characters between the slashes (/); the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

Before removing a directory, you must first delete all of the files in the directory.

The device prompts you for confirmation before deleting each directory.

Example

This example shows how to remove a directory:

```
Device: rmdir usbflash0:Test
```

You can verify that the directory was deleted by entering the **dir** *filesystem:* boot loader command.

sdm prefer

To specify the SDM template for use on the switch, use the **sdm prefer** command in global configuration mode.

sdm prefer
{**advanced**}

Syntax Description

advanced	Supports advanced features such as NetFlow.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

In a stack, all stack members must use the same SDM template that is stored on the active .

When a new is added to a stack, the SDM configuration that is stored on the active overrides the template configured on an individual .

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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

Command	Description
show parser encrypt file status	Displays the private configuration encryption status.

set

To set or display environment variables, use the **set** command in boot loader mode. Environment variables can be used to control the boot loader or any other software running on the device.

set *variable value*

Syntax Description

variable value	Use one of the following keywords for *variable* and the appropriate value for *value*: **MANUAL_BOOT**—Decides whether the device 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.
	BOOT *filesystem:/file-url*—Identifies a semicolon-separated list of executable files to try to load and execute when automatically booting. If the BOOT environment variable is not set, the system attempts to load and execute the first executable image it can find by using a recursive, depth-first search through the flash: file system. If the BOOT variable is set but the specified images cannot be loaded, the system attempts to boot the first bootable file that it can find in the flash: file system.
	ENABLE_BREAK—Allows the automatic boot process to be interrupted when the user presses the **Break** key on the console. Valid values are 1, Yes, On, 0, No, and Off. If set to 1, Yes, or On, you can interrupt the automatic boot process by pressing the **Break** key on the console after the flash: file system has initialized.
	HELPER *filesystem:/file-url*—Identifies a semicolon-separated list of loadable files to dynamically load during the boot loader initialization. Helper files extend or patch the functionality of the boot loader.
	PS1 *prompt*—Specifies a string that is used as the command-line prompt in boot loader mode.
	CONFIG_FILE flash: */file-url*—Specifies the filename that Cisco IOS uses to read and write a nonvolatile copy of the system configuration.
	BAUD *rate*—Specifies the number of bits per second (b/s) that is used for the baud rate for the console. The Cisco IOS software inherits the baud rate setting from the boot loader and continues to use this value unless the configuration file specifies another setting. The range is from 0 to 128000 b/s. Valid values are 50, 75, 110, 150, 300, 600, 1200, 1800, 2000, 2400, 3600, 4800, 7200, 9600, 14400, 19200, 28800, 38400, 56000, 57600, 115200, and 128000. The most commonly used values are 300, 1200, 2400, 9600, 19200, 57600, and 115200.
	SWITCH_NUMBER *stack-member-number*—Changes the member number of a stack member.
	SWITCH_PRIORITY *priority-number*—Changes the priority value of a stack member.

Command Default

The environment variables have these default values:

MANUAL_BOOT: No (0)

BOOT: Null string

ENABLE_BREAK: No (Off or 0) (the automatic boot process cannot be interrupted by pressing the **Break** key on the console).

HELPER: No default value (helper files are not automatically loaded).

PS1 device:

CONFIG_FILE: config.text

BAUD: 9600 b/s

SWITCH_NUMBER: 1

SWITCH_PRIORITY: 1

Note Environment variables that have values are stored in the flash: file system in various files. Each line in the files contains an environment variable name and an equal sign followed by the value of the variable.

A variable has no value if it is not listed in these files; it has a value if it is listed even if the value is a null string. A variable that is set to a null string (for example, " ") is a variable with a value.

Many environment variables are predefined and have default values.

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Environment variables are case sensitive and must be entered as documented.

Environment variables that have values are stored in flash memory outside of the flash: file system.

Under typical circumstances, it is not necessary to alter the setting of the environment variables.

The MANUAL_BOOT environment variable can also be set by using the **boot manual** global configuration command.

The BOOT environment variable can also be set by using the **boot system** *filesystem:/file-url* global configuration command.

The ENABLE_BREAK environment variable can also be set by using the **boot enable-break** global configuration command.

The HELPER environment variable can also be set by using the **boot helper** *filesystem: / file-url* global configuration command.

The CONFIG_FILE environment variable can also be set by using the **boot config-file flash:** */file-url* global configuration command.

The SWITCH_NUMBER environment variable can also be set by using the **switch** *current-stack-member-number* **renumber** *new-stack-member-number* global configuration command.

The SWITCH_PRIORITY environment variable can also be set by using the device *stack-member-number* **priority** *priority-number* global configuration command.

The boot loader prompt string (PS1) can be up to 120 printable characters not including the equal sign (=).

Example

This example shows how to set the SWITCH_PRIORITY environment variable:

```
Device: set SWITCH_PRIORITY 2
```

You can verify your setting by using the **set** boot loader command.

show avc client

To display information about top number of applications, use the **show avc client** command in privileged EXEC mode.

show avc client *client-mac* **top** *n* **application** [**aggregate** | **upstream** | **downstream**]

Syntax Description

client *client-mac*	Specifies the client MAC address.
top *n* **application**	Specifies the number of top "N" applications for the given client.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
	This command was introduced.

The following is sample output from the **show avc client** command:

```
# sh avc client 0040.96ae.65ec top 10 application aggregate

Cumulative Stats:

No.  AppName      Packet-Count    Byte-Count       AvgPkt-Size     usage%
---------------------------------------------------------------------------
1    skinny          7343           449860           61              94
2    unknown         99             13631            137             3
3    dhcp            18             8752             486             2
4    http            18             3264             181             1
5    tftp            9              534              59              0
6    dns             2              224              112             0

Last Interval(90 seconds) Stats:

No.  AppName     Packet-Count     Byte-Count       AvgPkt-Size      usage%
---------------------------------------------------------------------------
1    skinny          9              540              60               100
```

show debug

To display all the debug commands available on a switch, use the **show debug** command in Privileged EXEC mode.

show debug

show debug condition *Condition identifier* | *All conditions*

Syntax Description

Condition identifier	Sets the value of the condition identifier to be used. Range is between 1 and 1000.
All conditions	Shows all conditional debugging options available.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Release 16.1	This command was introduced.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use debug commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use debug commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased debug command processing overhead will affect system use.

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 xps

To display budgeting, configuration, power, and system power information for the Cisco eXpandable Power System (XPS) 2200, use the **show env xps** command in privileged EXEC mode.

show env xps { **budgeting** | **configuration** | **port** [**all** | *number*] | **power** | **system** | **thermal** | **upgrade** | **version** }

Syntax Description

budgeting	Displays XPS power budgeting, the allocated and budgeted power of all switches in the power stack.
configuration	Displays the configuration resulting from the power xps privileged EXEC commands. The XPS configuration is stored in the XPS. Enter the show env xps configuration command to retrieve the non-default configuration.
port [**all** | *number*]	Displays the configuration and status of all ports or the specified XPS port. Port numbers are from 1 to 9.
power	Displays the status of the XPS power supplies.
system	Displays the XPS system status.
thermal	Displays the XPS thermal status.
upgrade	Displays the XPS upgrade status.
version	Displays the XPS version details.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(55)SE1	This command was introduced.

Usage Guidelines

Use the **show env xps** privileged EXEC command to display the information for XPS 2200.

Examples

This is an example of output from the show env xps budgeting command:

```
Switch#
=======


XPS 0101.0100.0000 :
============================================================
Data                 Current    Power     Power Port  Switch #  PS A  PS B  Role-State
Committed
Budget
----  --------  ----  ----  ---------- ---------  ------ 1     -        -    715  SP-PS
   223
    1543
```

```
2     -        -    -    SP-PS      223       223
3     -        -    -    -          -         -
4     -        -    -    -          -         -
5     -        -    -    -          -         -
6     -        -    -    -          -         -
7     -        -    -    -          -         -
8     -        -    -    -          -         -
9     1        1100 -    RPS-NB     223        070
XPS  -        -    1100  -          -
```

This is an example of output from the show env xps configuration command:

```
Switch# show env xps configuration
==========================================
XPS 0101.0100.0000 :
==========================================
power xps port 4 priority 5
power xps port 5 mode disable
power xps port 5 priority 6
power xps port 6 priority 7
power xps port 7 priority 8
power xps port 8 priority 9
power xps port 9 priority 4
```

This is an example of output from the show env xps port all command:

```
Switch#
XPS 010



----------------------------------------
Port name          : -
Connected          : Yes
Mode               : Enabled (On)
Priority           : 1
Data stack switch # : - Configured role    : Auto-SP
Run mode            : SP-PS : Stack Power Power-Sharing Mode
Cable faults        : 0x0 XPS 0101.0100.0000 Port 2
----------------------------------------
Port name          : -
Connected          : Yes
Mode               : Enabled (On)
Priority           : 2
Data stack switch # : - Configured role    : Auto-SP
Run mode            : SP-PS : Stack Power Power-Sharing Mode
Cable faults        : 0x0 XPS 0101.0100.0000 Port 3
----------------------------------------
Port name          : -
Connected          : No
Mode               : Enabled (On)
Priority           : 3
Data stack switch # : - Configured role    : Auto-SP Run mode           : -
Cable faults
<output truncated>
```

This is an example of output from the show env xps power command:

```
================================================================================
XPS 0101.0100.0000 :
================================================================================
Port-Supply SW PID                 Serial#     Status         Mode Watts
----------- -- ------------------  ----------- --------------  ----  -----
XPS-A           Not present
XPS-B           NG3K-PWR-1100WAC   LIT13320NTV OK             SP   1100
1-A         -  -                   -           -
```

```
1-B         -  -                    -           -               SP    715
2-A         -  -                    -           -
2-B         -  -                    -           -
9-A                       100WAC    LIT141307RK OK              RPS  1100
9-B                   esent
```

This is an example of output from the show env xps system command:

```
Switch#
=======


XPS 0101.0100.0000 :
================================================================================
XPS                         Cfg  Cfg      RPS Switch  Current    Data Port  XPS Port Name

Mode Role    Pri Conn    Role-State  Switch #
----  --------------------  ---- -------  --- ------  ----------  --------
1     -                     On   Auto-SP  1   Yes     SP-PS      -
2     -                     On   Auto-SP  2   Yes     SP-PS      -
3     -                     On   Auto-SP  3   No      -          -
4     none                  On   Auto-SP  5   No      -          -
5     -                     Off  Auto-SP  6   No      -          -
6     -                     On   Auto-SP  7   No      -          -
7     -                     On   Auto-SP  8   No      -          -
8     -                     On   Auto-SP  9   No      -
9     test                  On   Auto-SP  4   Yes     RPS-NB
```

This is an example of output from the show env xps thermal command:

```
Switch#
=======


XPS 0101.0100.0000 :
============================================
Fan  Status
----  -----------
1     OK
2     OK
3     NOT PRESENT PS-1  NOT PRESENT PS-2  OK Temperature is OK
```

This is an example of output from the show env xps upgrade command when no upgrade is occurring:

```
Switch# show env xps upgrade
No XPS is connected and upgrading.
```

These are examples of output from the show env xps upgrade command when an upgrade is in process:

```
Switch# show env xps upgrade
XPS Upgrade Xfer

SW Status Prog
-- ----------- ----
1 Waiting 0%
Switch#
*Mar 22 03:12:46.723: %PLATFORM_XPS-6-UPGRADE_START: XPS 0022.bdd7.9b14 upgrade has
started through the Service Port.
Switch# show env xps upgrade
XPS Upgrade Xfer
SW Status Prog
-- ----------- ----
1 Receiving 1%
Switch# show env xps upgrade
```

```
XPS Upgrade Xfer
SW Status Prog
-- ----------- ----
1 Receiving 5%
Switch# show env xps upgrade
XPS Upgrade Xfer
SW Status Prog
-- ----------- ----
1 Reloading 100%
Switch#
*Mar 22 03:16:01.733: %PLATFORM_XPS-6-UPGRADE_DONE: XPS 0022.bdd7.9b14 upgrade has
completed and the XPS is reloading.
```

This is an example of output from the show env xps version command:

```
Switch# show env xps version
==========================================
XPS 0022.bdd7.9b14:
==========================================
Serial Number: FDO13490KUT
Hardware Version: 8
Bootloader Version: 7
Software Version: 18
```

Table 149: Related Commands

Command	Description
power xps(global configuration command)	Configures XPS and XPS port names.
power xps(privileged EXEC command)	Configures the XPS ports and system.

show flow monitor

To display the status and statistics for a Flexible NetFlow flow monitor, use the **show flow monitor** command in privileged EXEC mode.

show flow monitor [{**broker** [{**detail** | **picture**}] | [**name**] *monitor-name* [{**cache** [**format** {**csv** | **record** | **table**}]}] | **provisioning** | **statistics**}]

Syntax Description

broker	(Optional) Displays information about the state of the broker for the flow monitor
detail	(Optional) Displays detailed information about the flow monitor broker.
picture	(Optional) Displays a picture of the broker state.
name	(Optional) Specifies the name of a flow monitor.
monitor-name	(Optional) Name of a flow monitor that was previously configured.
cache	(Optional) Displays the contents of the cache for the flow monitor.
format	(Optional) Specifies the use of one of the format options for formatting the display output.
csv	(Optional) Displays the flow monitor cache contents in comma-separated variables (CSV) format.
record	(Optional) Displays the flow monitor cache contents in record format.
table	(Optional) Displays the flow monitor cache contents in table format.
provisioning	(Optional) Displays the flow monitor provisioning information.
statistics	(Optional) Displays the statistics for the flow monitor.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The **cache** keyword uses the record format by default.

The uppercase field names in the display output of the **show flowmonitor** *monitor-name* **cache** command are key fields that Flexible NetFlow uses to differentiate flows. The lowercase field names in the display output of the **show flow monitor** *monitor-name* **cache** command are nonkey fields from which Flexible NetFlow collects values as additional data for the cache.

Examples

The following example displays the status for a flow monitor:

```
# show flow monitor FLOW-MONITOR-1

Flow Monitor FLOW-MONITOR-1:
  Description:       Used for basic traffic analysis
```

```
Flow Record:       flow-record-1
Flow Exporter:     flow-exporter-1
                   flow-exporter-2
Cache:
  Type:              normal
  Status:            allocated
  Size:              4096 entries / 311316 bytes
  Inactive Timeout:  15 secs
  Active Timeout:    1800 secs
  Update Timeout:    1800 secs
```

This table describes the significant fields shown in the display.

Table 150: show flow monitor monitor-name Field Descriptions

Field	Description
Flow Monitor	Name of the flow monitor that you configured.
Description	Description that you configured or the monitor, or the default description User defined.
Flow Record	Flow record assigned to the flow monitor.
Flow Exporter	Exporters that are assigned to the flow monitor.
Cache	Information about the cache for the flow monitor.
Type	Flow monitor cache type. The possible values are: • immediate—Flows are expired immediately. • normal—Flows are expired normally. • Permanent—Flows are never expired.
Status	Status of the flow monitor cache. The possible values are: • allocated—The cache is allocated. • being deleted—The cache is being deleted. • not allocated—The cache is not allocated.
Size	Current cache size.
Inactive Timeout	Current value for the inactive timeout in seconds.
Active Timeout	Current value for the active timeout in seconds.
Update Timeout	Current value for the update timeout in seconds.

The following example displays the status, statistics, and data for the flow monitor named FLOW-MONITOR-1:

```
# show flow monitor FLOW-MONITOR-1 cache
  Cache type:                               Normal (Platform cache)
  Cache size:                              Unknown
  Current entries:                               1

  Flows added:                                   3
  Flows aged:                                    2
    - Active timeout      (   300 secs)          2

DATALINK MAC SOURCE ADDRESS INPUT:       0000.0000.1000
DATALINK MAC DESTINATION ADDRESS INPUT:  6400.F125.59E6
IPV6 SOURCE ADDRESS:                     2001:DB8::1
IPV6 DESTINATION ADDRESS:                2001:DB8:1::1
TRNS SOURCE PORT:                        1111
TRNS DESTINATION PORT:                   2222
IP VERSION:                              6
IP PROTOCOL:                             6
IP TOS:                                  0x05
IP TTL:                                  11
tcp flags:                               0x20
counter bytes long:                      132059538
counter packets long:                    1158417
```

This table describes the significant fields shown in the display.

Table 151: show flow monitor monitor-name cache Field Descriptions

Field	Description
Cache type	Flow monitor cache type. The value is always normal, as it is the only supported cache type.
Cache Size	Number of entries in the cache.
Current entries	Number of entries in the cache that are in use.
Flows added	Flows added to the cache since the cache was created.
Flows aged	Flows expired from the cache since the cache was created.
Active timeout	Current value for the active timeout in seconds.
Inactive timeout	Current value for the inactive timeout in seconds.
DATALINK MAC SOURCE ADDRESS INPUT	MAC source address of input packets.
DATALINK MAC DESTINATION ADDRESS INPUT	MAC destination address of input packets.
IPV6 SOURCE ADDRESS	IPv6 source address.
IPV6 DESTINATION ADDRESS	IPv6 destination address.
TRNS SOURCE PORT	Source port for the transport protocol.
TRNS DESTINATION PORT	Destination port for the transport protocol.

Field	Description
IP VERSION	IP version.
IP PROTOCOL	Protocol number.
IP TOS	IP type of service (ToS) value.
IP TTL	IP time-to-live (TTL) value.
tcp flags	Value of the TCP flags.
counter bytes	Number of bytes that have been counted.
counter packets	Number of packets that have been counted.

The following example displays the status, statistics, and data for the flow monitor named FLOW-MONITOR-1 in a table format:

```
# show flow monitor FLOW-MONITOR-1 cache format table
  Cache type:                               Normal (Platform cache)
  Cache size:                              Unknown
  Current entries:                               1

  Flows added:                                   3
  Flows aged:                                    2
    - Active timeout      (   300 secs)          2

DATALINK MAC SRC ADDR INPUT  DATALINK MAC DST ADDR INPUT  IPV6 SRC ADDR  IPV6 DST ADDR
TRNS SRC PORT  TRNS DST PORT  IP VERSION  IP PROT  IP TOS  IP TTL  tcp flags  bytes long
pkts long
============================  ============================  =============  =============
=============  =============  ==========  =======  ======  ======  =========  ==========
=========
0000.0000.1000               6400.F125.59E6               2001:DB8::1    2001:DB8:1::1
       1111           2222           6        6  0x05        11  0x20        132059538
1158417
```

The following example displays the status, statistics, and data for the flow monitor named FLOW-MONITOR-IPv6 (the cache contains IPv6 data) in record format:

```
# show flow monitor name FLOW-MONITOR-IPv6 cache format record
  Cache type:                                Normal (Platform cache)
  Cache size:                               Unknown
  Current entries:                                1

  Flows added:                                    3
  Flows aged:                                     2
    - Active timeout      (   300 secs)           2

DATALINK MAC SOURCE ADDRESS INPUT:       0000.0000.1000
DATALINK MAC DESTINATION ADDRESS INPUT:  6400.F125.59E6
IPV6 SOURCE ADDRESS:                     2001::2
IPV6 DESTINATION ADDRESS:                2002::2
TRNS SOURCE PORT:                        1111
TRNS DESTINATION PORT:                   2222
IP VERSION:                              6
IP PROTOCOL:                             6
IP TOS:                                  0x05
IP TTL:                                  11
tcp flags:                               0x20
```

```
counter bytes long:                     132059538
counter packets long:                   1158417
```

The following example displays the status and statistics for a flow monitor:

```
# show flow monitor FLOW-MONITOR-1 statistics
  Cache type:                               Normal (Platform cache)
  Cache size:                              Unknown
  Current entries:                               1

  Flows added:                                   3
  Flows aged:                                    2
    - Active timeout      (   300 secs)          2
```

show 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

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines

Use the show commands to view the status of the install package.

Example

The following is sample output from the **show install package** command:

```
Device# show install package bootflash: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 152: show install summary Field Descriptions

Field	Description
Active Packages	Name of the active install package.
Inactive Packages	List of inactive packages.
Committed Packages	Install packages that have saved or committed changes to the harddisk, so that the changes become persistent across reloads.
Uncommitted Packages	Intall package activations that are nonpersistent.

The following is sample output from the **show install log** command:

```
Device# show install log

[0|install_op_boot]: START Fri Feb 24 19:20:19 Universal 2017
[0|install_op_boot]: END SUCCESS  Fri Feb 24 19:20:23 Universal 2017
[3|install_add]: START Sun Feb 26 05:55:31 UTC 2017
[3|install_add( FATAL)]: File path (scp) is not yet supported for this command
[4|install_add]: START Sun Feb 26 05:57:04 UTC 2017
[4|install_add]: END SUCCESS
/bootflash/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

Command	Description
install	Installs SMU packages.

show license all

To display the entitlement information, use the **show license all** command in privileged EXEC mode.

show license all

Syntax Description

This command has no arguments or keywords.

Command Default

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.1	This command was introduced.

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 allSmart Licensing Status
======================

Smart Licensing is ENABLED

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 14:49:48 2019 IST
  Registration Expires: Jul 19 14:43:48 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

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
==============
```

```
C9200L DNA Advantage, 48-port Term license (C9200L-DNA-A-48):
  Description: C9200L DNA Advantage, 48-port Term license
  Count: 1
  Version: 1.0
  Status: AUTHORIZED

C9200L Network Advantage, 48-port license (C9200L-NW-A-48):
  Description: C9200L Network Advantage, 48-port license
  Count: 1
  Version: 1.0
  Status: AUTHORIZED

Product Information
===================
UDI: PID:C9200L-48P-4X,SN:JPG221300KP

Agent Version
=============
Smart Agent for Licensing: 4.4.13_rel/116
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
```

Related Commands

Command	Description
show license status	Displays compliance status of a license.
show license summary	Displays summary of all active licenses.
show license udi	Displays UDI.
show license usage	Displays license usage information
show tech-support license	Displays the debug output.

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

Release	Modification
Cisco IOS XE Fuji 16.9.1	This command was introduced.

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

Command	Description
show license all	Displays entitlements information.

Command	Description
show license summary	Displays summary of all active licenses.
show license udi	Displays UDI.
show license usage	Displays license usage information
show tech-support license	Displays the debug output.

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

Release	Modification
Cisco IOS XE Fuji 16.9.1	This command was introduced.

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: SUCCEEDED
  Next Renewal Attempt: Jan 15 14:49:48 2019 IST

License Authorization:
  Status: AUTHORIZED
  Last Communication Attempt: SUCCEEDED
  Next Communication Attempt: Aug 27 07:02:56 2018 IST

License Usage:
  License                 Entitlement tag               Count Status
  -----------------------------------------------------------------------------
  C9200L DNA Advantage... (C9200L-DNA-A-48)                 1 AUTHORIZED
  C9200L Network Advan... (C9200L-NW-A-48)                  1 AUTHORIZED
```

Related Commands

Command	Description
show license all	Displays entitlements information.
show license status	Displays compliance status of a license.
show license udi	Displays UDI.
show license usage	Displays license usage information
show tech-support license	Displays the debug output.

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

Release	Modification
Cisco IOS XE Fuji 16.9.1	This command was introduced.

Example

This example shows a sample output from the **show license udi** command:

```
Device# show license udi
UDI: PID:C9200L-48P-4X,SN:JPG221300KP
```

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

Privileged EXEC (#)

Release	Modification
Cisco IOS XE Fuji 16.9.1	This command was introduced.

Example

This example shows a sample output from the **show license usage** command:

```
Device# show license usage
License Authorization:
  Status: AUTHORIZED on Jul 28 07:02:56 2018 IST

C9200L DNA Advantage, 48-port Term license (C9200L-DNA-A-48):
  Description: C9200L DNA Advantage, 48-port Term license
  Count: 1
  Version: 1.0
  Status: AUTHORIZED

C9200L Network Advantage, 48-port license (C9200L-NW-A-48):
  Description: C9200L Network Advantage, 48-port license
  Count: 1
  Version: 1.0
  Status: AUTHORIZED
```

Related Commands

Command	Description
show license all	Displays entitlements information.
show license status	Displays compliance status of a license.
show license summary	Displays summary of all active licenses.
show license udi	Displays UDI.
show tech-support license	Displays the debug output.

show location

To display location information for an endpoint, use the **show location** command in privileged EXEC mode.

show location
[{**admin-tag** | **civic-location**{**identifier** *identifier-string* | **interface** *type number* | **static**} | **custom-location**{**identifier** *identifier-string* | **interface** *type number* | **static**} | **elin-location**{**identifier** *identifier-string* | **interface** *type number* | **static**} | **geo-location**{**identifier** *identifier-string* | **interface** *type number* | **static**} | **host**}]

Syntax Description

admin-tag	Displays administrative tag or site information.
civic-location	Specifies civic location information.
identifier *identifier-string*	Information identifier of the civic location, custom location, or geo-spatial location.
interface *type number*	Interface type and number. For information about the numbering syntax for your device, use the question mark (?) online help function.
static	Displays configured civic, custom, or geo-spatial location information.
custom-location	Specifies custom location information.
elin-location	Specifies emergency location information (ELIN).
geo-location	Specifies geo-spatial location information.
host	Specifies the civic, custom, or geo-spatial host location information.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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
```

```
City                        : San Jose
State                       : CA
Country                     : US
```

Related Commands

Command	Description
location	Configures location information for an endpoint.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was implemented on the Cisco Catalyst 9200 Series Switches
Cisco IOS XE Gibraltar 16.10.1	The output of this command was updated to display the reload reasons for members in a stack.

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
```

```
06/18/2018 19:40:30   Reload                          0     0     0     0     5
06/18/2018 20:37:47   Reload                          0     0     0     0     5
06/18/2018 20:51:13   Reload                          0     0     0     0     5
06/18/2018 21:04:08   Reload                          0     0     0     0     5
06/18/2018 21:18:23   Reload                          0     0     0     0     5
06/18/2018 21:31:25   Reload                          0     0     0     0     5
06/18/2018 21:45:15   Reload                          0     0     0     0     5
06/18/2018 21:59:02   Reload                          0     0     0     0     5
06/18/2018 22:11:41   Reload                          0     0     0     0     5
06/18/2018 22:24:27   Reload                          0     0     0     0     5
06/18/2018 22:39:14   Reload Command                  0     0     0     0     4
06/19/2018 00:01:59   Reload Command                  0     0     0     1     5
06/19/2018 00:13:21   redundancy force-switchover     0     0     0     0     5
06/19/2018 01:05:42   redundancy force-switchover     0     0     0     0     5
06/20/2018 02:37:16   redundancy force-switchover     0     0     1     1     5
06/20/2018 02:50:03   redundancy force-switchover     0     0     0     0     5
06/20/2018 03:02:13   redundancy force-switchover     0     0     0     0     5
06/20/2018 03:14:26   redundancy force-switchover     0     0     0     0     5
06/20/2018 03:26:44   redundancy force-switchover     0     0     0     0     5
06/20/2018 03:38:58   redundancy force-switchover     0     0     0     0     5
06/20/2018 03:52:43   redundancy force-switchover     0     0     0     0     5
06/20/2018 04:05:16   redundancy force-switchover     0     0     0     0     5
.
.
.
```

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 reset timestamp : 09/17/2018 10:59:57
Current slot            : 1
Chassis type            : 0
Current uptime          :  0  years  0  weeks  0  days  0  hours  0  minutes
----------------------------------------------------------------------------

----------------------------------------------------------------------------
UPTIME CONTINUOUS INFORMATION
----------------------------------------------------------------------------
Time Stamp          | Reset                       | Uptime
MM/DD/YYYY HH:MM:SS | Reason                      | years weeks days hours minutes
----------------------------------------------------------------------------
06/10/2017 09:28:22   Reload                          0     0     0     0     0
<snip>
09/17/2018 09:07:44   PowerOn                         0     0     3     15    5
09/17/2018 10:16:26   Reload Command                  0     0     0     1     5
09/17/2018 10:59:57   PowerOn                         0     0     0     0     5
```

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
----------------------------------------------------------------------------
```

```
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 reset timestamp : 09/17/2018 10:59:57
Current slot            : 2
Chassis type            : 0
Current uptime          :  0  years  0  weeks  0  days  0  hours  5  minutes
-------------------------------------------------------------------------------

-------------------------------------------------------------------------------
UPTIME CONTINUOUS INFORMATION
-------------------------------------------------------------------------------
Time Stamp          | Reset                        | Uptime
MM/DD/YYYY HH:MM:SS | Reason                       | years weeks days hours minutes
-------------------------------------------------------------------------------
06/10/2017 11:51:26   Reload                         0     0     0     0     0
<snip>
08/10/2018 09:13:58   LocalSoft                      0     0     2     5     4
08/28/2018 14:21:42   Reload Slot Command            0     0     0     3     5
08/28/2018 14:34:29   System requested reload        0     0     0     0     0
09/11/2018 09:08:15   Reload                         0     0     1     8     5
09/11/2018 19:15:06   redundancy force-switchover    0     0     0     9     4
09/13/2018 16:50:18   Reload Command                 0     0     1     21    6
09/17/2018 10:55:09   PowerOn                        0     0     0     0     5
```

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
-------------------------------------------------------------------------------
```

show mac address-table

To display the MAC address table, use the **show mac address-table** command in privileged EXEC mode.

show mac address-table [{ **address** *mac-addr* [**interface** *type/number* | **vlan** *vlan-id*] | **aging-time** [**routed-mac** | **vlan** *vlan-id*] | **control-packet-learn** | **count** [**summary** | **vlan** *vlan-id*] | [**dynamic** | **secure** | **static**] [**address** *mac-addr*] [**interface** *type/number* | **vlan** *vlan-id*] | **interface** *type/number* | **learning** [**vlan** *vlan-id*] | **multicast** [**count**] [**igmp-snooping** | **mld-snooping** | **user**] [**vlan** *vlan-id*] | **notification** { **change** [**interface** [*type/number*]] | **mac-move** | **threshold** } | **vlan** *vlan-id* }]

Syntax Description

address *mac-addr*	(Optional) Displays information about the MAC address table for a specific MAC address.
interface *type/number*	(Optional) Displays addresses for a specific interface.
vlan *vlan-id*	(Optional) Displays addresses for a specific VLAN.
aging-time [**routed-mac** | **vlan** *vlan-id*]	(Optional) Displays the aging time for the routed MAC or VLAN.
control-packet-learn	(Optional) Displays the controlled packet MAC learning parameters.
count	(Optional) Displays the number of entries that are currently in the MAC address table.
dynamic	(Optional) Displays only the dynamic addresses.
secure	(Optional) Displays only the secure addresses.
static	(Optional) Displays only the static addresses.
learning	(Optional) Displays learnings of a VLAN or interface.
multicast	(Optional) Displays information about the multicast MAC address table entries only.
igmp-snooping	(Optional) Displays the addresses learned by Internet Group Management Protocol (IGMP) snooping.
mld-snooping	(Optional) Displays the addresses learned by Multicast Listener Discover version 2 (MLDv2) snooping.
user	(Optional) Displays the manually entered (static) addresses.
notification change	Displays the MAC notification parameters and history table.
notification mac-move	Displays the MAC-move notification status.
notification threshold	Displays the Counter-Addressable Memory (CAM) table utilization notification status.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.
Cisco IOS XE Gibraltar 16.12.4	The ouput of the **show mac address-table vlan** *vlan-id* command has been updated to show the MAC addresses used for Cisco Software-Defined Access (SD-Access) solution.

Usage Guidelines

The *mac-addr* value is a 48-bit MAC address. The valid format is H.H.H.

The interface *number* argument designates the module and port number. Valid values depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

The following is sample output from the **show mac address-table** command:

```
Device# show mac address-table

          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 All    0100.0ccc.cccc    STATIC      CPU
 All    0100.0ccc.cccd    STATIC      CPU
 All    0180.c200.0000    STATIC      CPU
 All    0180.c200.0001    STATIC      CPU
 All    0180.c200.0002    STATIC      CPU
 All    0180.c200.0003    STATIC      CPU
 All    0180.c200.0004    STATIC      CPU
 All    0180.c200.0005    STATIC      CPU
 All    0180.c200.0006    STATIC      CPU
 All    0180.c200.0007    STATIC      CPU
 All    0180.c200.0008    STATIC      CPU
 All    0180.c200.0009    STATIC      CPU
 All    0180.c200.000a    STATIC      CPU
 All    0180.c200.000b    STATIC      CPU
 All    0180.c200.000c    STATIC      CPU
 All    0180.c200.000d    STATIC      CPU
 All    0180.c200.000e    STATIC      CPU
 All    0180.c200.000f    STATIC      CPU
 All    0180.c200.0010    STATIC      CPU
 All    0180.c200.0021    STATIC      CPU
 All    ffff.ffff.ffff    STATIC      CPU
   1    780c.f0e1.1dc3    STATIC      Vl1
  51    0000.1111.2222    STATIC      Vl51
  51    780c.f0e1.1dc6    STATIC      Vl51
1021    0000.0c9f.f45c    STATIC      Vl1021
1021    0002.02cc.0002    STATIC      Gi6/0/2
1021    0002.02cc.0003    STATIC      Gi6/0/3
1021    0002.02cc.0004    STATIC      Gi6/0/4
1021    0002.02cc.0005    STATIC      Gi6/0/5
1021    0002.02cc.0006    STATIC      Gi6/0/6
1021    0002.02cc.0007    STATIC      Gi6/0/7
1021    0002.02cc.0008    STATIC      Gi6/0/8
1021    0002.02cc.0009    STATIC      Gi6/0/9
1021    0002.02cc.000a    STATIC      Gi6/0/10
```

```
<output truncated>
```

The following example shows how to display MAC address table information for a specific MAC address:

```
Device# show mac address-table address fc58.9a02.7382

          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    fc58.9a02.7382    DYNAMIC     Te1/0/1
Total Mac Addresses for this criterion: 1
```

The following example shows how to display the currently configured aging time for a specific VLAN:

```
Device# show mac address-table aging-time vlan 1

Global Aging Time:  300
Vlan    Aging Time
----    ----------
   1     300
```

The following example shows how to display the information about the MAC address table for a specific interface:

```
Device# show mac address-table interface TenGigabitEthernet1/0/1

          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    fc58.9a02.7382    DYNAMIC     Te1/0/1
Total Mac Addresses for this criterion: 1
```

The following example shows how to display the MAC-move notification status:

```
Device# show mac address-table notification mac-move

MAC Move Notification: Enabled
```

The following example shows how to display the CAM-table utilization-notification status:

```
Device# show mac address-table notification threshold

    Status       limit        Interval
-------------+-----------+-------------
   enabled         50           120
```

The following example shows how to display the MAC notification parameters and history table for a specific interface:

```
Device# show mac address-table notification change interface tenGigabitEthernet1/0/1

MAC Notification Feature is Disabled on the switch
Interface                       MAC Added Trap MAC Removed Trap
---------                       -------------- ----------------
```

```
TenGigabitEthernet1/0/1        Disabled       Disabled
```

The following example shows how to display the information about the MAC-address table for a specific VLAN:

Note MAC addresses of the type CP_LEARN will be displayed only if Cisco SD-Access solution is used.

```
Device# show mac address-table vlan 1021

          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
1021    0000.0c9f.f45c    STATIC      Vl1021
1021    0002.02cc.0002    STATIC      Gi6/0/2
1021    0002.02cc.0003    STATIC      Gi6/0/3
1021    0002.02cc.0004    STATIC      Gi6/0/4
1021    0002.02cc.0005    STATIC      Gi6/0/5
1021    0002.02cc.0006    STATIC      Gi6/0/6
1021    0002.02cc.0007    STATIC      Gi6/0/7
1021    0002.02cc.0008    STATIC      Gi6/0/8
1021    0002.02cc.0009    STATIC      Gi6/0/9
1021    0002.02cc.000a    STATIC      Gi6/0/10
1021    0002.02cc.000b    STATIC      Gi6/0/11
1021    0002.02cc.000c    STATIC      Gi6/0/12
1021    0002.02cc.000d    STATIC      Gi6/0/13
1021    0002.02cc.000e    STATIC      Gi6/0/14
1021    0002.02cc.000f    STATIC      Gi6/0/15
1021    0002.02cc.0010    STATIC      Gi6/0/16
1021    0002.02cc.0011    STATIC      Gi6/0/17
1021    0002.02cc.0012    STATIC      Gi6/0/18
1021    0002.02cc.0013    STATIC      Gi6/0/19
1021    0002.02cc.0014    STATIC      Gi6/0/20

.
.
.

1021    0002.0100.0001    CP_LEARN    Tu0
1021    0002.0100.0002    CP_LEARN    Tu0
1021    0002.0100.0003    CP_LEARN    Tu0
1021    0002.0100.0004    CP_LEARN    Tu0
1021    0002.0100.0005    CP_LEARN    Tu0
1021    0002.0100.0006    CP_LEARN    Tu0
1021    0002.0100.0007    CP_LEARN    Tu0
1021    0002.0100.0008    CP_LEARN    Tu0
1021    0002.0100.0009    CP_LEARN    Tu0
1021    0002.0100.000a    CP_LEARN    Tu0
Total Mac Addresses for this criterion: 114
```

The table below describes the significant fields shown in the **show mac address-table** display.

Table 153: show mac address-table Field Descriptions

Field	Description
VLAN	VLAN number.
Mac Address	MAC address of the entry.
Type	Type of address.
Ports	Port type.
Total MAC addresses	Total MAC addresses in the MAC address table.

Related Commands

Command	Description
clear mac address-table	Deletes dynamic entries from the MAC address table.

show mac address-table move update

To display the MAC address-table move update information on the device, use the **show mac address-table move update** command in EXEC mode.

show mac address-table move update

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

User EXEC

Privileged EXEC

Command History

Release
Cisco IOS XE Fuji 16.9.2

Example

This example shows the output from the **show mac address-table move update** command:

```
Device# show mac address-table move update

Switch-ID : 010b.4630.1780
Dst mac-address : 0180.c200.0010
Vlans/Macs supported : 1023/8320
Default/Current settings: Rcv Off/On, Xmt Off/On
Max packets per min : Rcv 40, Xmt 60
Rcv packet count : 10
Rcv conforming packet count : 5
Rcv invalid packet count : 0
Rcv packet count this min : 0
Rcv threshold exceed count : 0
Rcv last sequence# this min : 0
Rcv last interface : Po2
Rcv last src-mac-address : 0003.fd6a.8701
Rcv last switch-ID : 0303.fd63.7600
Xmt packet count : 0
Xmt packet count this min : 0
Xmt threshold exceed count : 0
Xmt pak buf unavail cnt : 0
Xmt last interface : None
```

show 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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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

Command	Description
service private-config-encryption	Enables private configuration file encryption.

show platform integrity

To display checksum record for the boot stages , use the **show platform integrity** command in privileged EXEC mode.

show platform integrity [**sign** [**nonce** <*nonce*>]]

Syntax Description

sign	(Optional) Show signature
nonce	(Optional) Enter a nonce value

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
	This command was introduced.

Examples

This example shows how to view the checksum record for boot stages :

```
Device# show platform integrity sign

PCR0: EE47F8644C2887D9BD4DE3E468DD27EB93F4A606006A0B7006E2928C50C7C9AB
PCR8: E7B61EC32AFA43DA1FF4D77F108CA266848B32924834F5E41A9F6893A9CB7A38
Signature version: 1
Signature:
816C5A29741BBAC1961C109FFC36DA5459A44DBF211025F539AFB4868EF91834C05789
5DAFBC7474F301916B7D0D08ABE5E05E66598426A73E921024C21504383228B6787B74
8526A305B17DAD3CF8705BACFD51A2D55A333415CABC73DAFDEEFD8777AA77F482EC4B
731A09826A41FB3EFFC46DC02FBA666534DBEC7DCC0C029298DB8462A70DBA26833C2A
1472D1F08D721BA941CB94A418E43803699174572A5759445B3564D8EAEE57D64AE304
EE1D2A9C53E93E05B24A92387E261199CED8D8A0CE7134596FF8D2D6E6DA773757C70C
D3BA91C43A591268C248DF32658999276FB972153ABE823F0ACFE9F3B6F0AD1A00E257
4A4CC41C954015A59FB8FE
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**}}}

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

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 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
type=AVC msg=audit(1539222292.586:101): 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(1539222292.586:102): avc:  denied  { read } for  pid=14028 comm="ls"
name="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(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(1539438600.897:120): avc:  denied  { execute_no_trans } for  pid=8300
comm="sh"
path="/tmp/sw/mount/cat9k-rpbase.2018-10-02_00.13_mhungund.SSA.pkg/nyquist/usr/bin/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
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  { 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
type=AVC msg=audit(1539438696.969:125): avc:  denied  { execute_no_trans } for  pid=10057
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(1539438732.973:126): 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(1539438778.008:127): 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(1539438800.156:128): 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
type=AVC msg=audit(1539438834.099:129): 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
type=AVC msg=audit(1539440246.697:149): 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
type=AVC msg=audit(1539440299.119:150): 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 ============
===================================
```

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_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
type=AVC msg=audit(1539222292.586:101): 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(1539222292.586:102): avc:  denied  { read } for  pid=14028 comm="ls"
name="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  { 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
type=AVC msg=audit(1539438696.969:125): avc:  denied  { execute_no_trans } for  pid=10057
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(1539438732.973:126): 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(1539438778.008:127): 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(1539438800.156:128): 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
type=AVC msg=audit(1539438834.099:129): 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
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 ============
===================================
```

show platform software fed switch punt cause

To display information about why the packets received on an interface are punted 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**}

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.
cause_id	Specifies the ID of the cause for which the details have to be displayed.
clear	Clears the statistics for all the causes. Clearing the causes might result in inconsistent statistics.
summary	Displays a high-level overview of the punt reason.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

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

Cause  Cause Info                     Rcvd                 Dropped
-------------------------------------------------------------------------------
7      ARP request or response         1                    0
21     RP<->QFP keepalive              22314                0
55     For-us control                  12                   0
60     IP subnet or broadcast packet   21                   0
96     Layer2 control protocols        133808               0
```

```
--------------------------------------------------------------------------------
```

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

Sub Cause       Rcvd                Dropped
-------------------------------------------
0               22363               0

-------------------------------------------
```

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 informtion.
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

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

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
==================================================================================
 Q  |         Queue            |  Rx    |  Rx   |  Rx    |  Drop  |  Drop   |  Drop
 no |         Name             |  prev  |  cur  |  delta |  prev  |  cur    |  delta
==================================================================================
 0  CPU_Q_DOT1X_AUTH                0        0        0        0        0        0
 1  CPU_Q_L2_CONTROL                0        6772     6772     0        0        0
 2  CPU_Q_FORUS_TRAFFIC             0        0        0        0        0        0
 3  CPU_Q_ICMP_GEN                  0        0        0        0        0        0
 4  CPU_Q_ROUTING_CONTROL           0        12       12       0        0        0
 5  CPU_Q_FORUS_ADDR_RESOLUTION     0        1        1        0        0        0
 6  CPU_Q_ICMP_REDIRECT             0        0        0        0        0        0
 7  CPU_Q_INTER_FED_TRAFFIC         0        0        0        0        0        0
 8  CPU_Q_L2LVX_CONTROL_PKT         0        0        0        0        0        0
 9  CPU_Q_EWLC_CONTROL              0        0        0        0        0        0
 10 CPU_Q_EWLC_DATA                 0        0        0        0        0        0
 11 CPU_Q_L2LVX_DATA_PKT            0        0        0        0        0        0
 12 CPU_Q_BROADCAST                 0        21       21       0        0        0
 13 CPU_Q_LEARNING_CACHE_OVFL       0        0        0        0        0        0
 14 CPU_Q_SW_FORWARDING             0        0        0        0        0        0
 15 CPU_Q_TOPOLOGY_CONTROL          0        127300   127300   0        0        0
 16 CPU_Q_PROTO_SNOOPING            0        0        0        0        0        0
 17 CPU_Q_BFD_LOW_LATENCY           0        0        0        0        0        0
 18 CPU_Q_TRANSIT_TRAFFIC           0        0        0        0        0        0
 19 CPU_Q_RPF_FAILED                0        0        0        0        0        0
 20 CPU_Q_MCAST_END_STATION_SERVICE 0        0        0        0        0        0
 21 CPU_Q_LOGGING                   0        0        0        0        0        0
 22 CPU_Q_PUNT_WEBAUTH              0        0        0        0        0        0
 23 CPU_Q_HIGH_RATE_APP             0        0        0        0        0        0
 24 CPU_Q_EXCEPTION                 0        0        0        0        0        0
 25 CPU_Q_SYSTEM_CRITICAL           0        0        0        0        0        0
 26 CPU_Q_NFL_SAMPLED_DATA          0        0        0        0        0        0
 27 CPU_Q_LOW_LATENCY               0        0        0        0        0        0
 28 CPU_Q_EGR_EXCEPTION             0        0        0        0        0        0
 29 CPU_Q_FSS                       0        0        0        0        0        0
 30 CPU_Q_MCAST_DATA                0        0        0        0        0        0
 31 CPU_Q_GOLD_PKT                  0        0        0        0        0        0

----------------------------------------------------------------------------------
```

The table below describes the significant fields shown in the display.

*Table 154: **show platform software fed switch active punt cpuq brief** Field Descriptions*

Field	Description
Q no	ID of the queue.
Queue Name	Name of the queue.
Rx	Number of packets received.

Field	Description
Drop	Number of packets dropped.

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.

show platform sudi certificate [**sign** [**nonce** <*nonce*>]]

Syntax Description

sign	(Optional) Show signature
nonce	(Optional) Enter a nonce value

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
	This command was introduced.

Examples

This example shows how to view the checksum record for a specific SUDI :

```
# show platform sudi certificate

-----BEGIN CERTIFICATE-----
MIIDQzCCAiugAwIBAgIQX/h7KCtU3I1CoxW1aMmt/zANBgkqhkiG9w0BAQUFADA1
MRYwFAYDVQQKEw1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENB
IDIwNDgwHhcNMDQwNTE0MjAxNzEyWhcNMjkwNTE0MjAyNTQyWjA1MRYwFAYDVQQK
Ew1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENBIDIwNDgwggEg
MA0GCSqGSIb3DQEBAQUAA4IBDQAwggEIAoIBAQCwmrmrp68Kd6ficba0ZmKUeIhH
xmJVhEAyv8CrLqUccda8bnuoqrpu0hWISEWdovyD0My5jOAmaHBKeN8hF570YQXJ
FcjPFto1YYmUQ6iEqDGYeJu5Tm8sUxJszR2tKyS7McQr/4NEb7Y9JHcJ6r8qqB9q
VvYgDxFUl4F1pyXOWWqCZe+36ufijXWLbvLdT6ZeYpzPEApk0E5tzivMW/VgpSdH
jWn0f84bcN5wGyDWbs2mAag8EtKpP6BrXruOIIt6keO1aO6g58QBdKhTCytKmg9l
Eg6CTY5j/e/rmxrbU6YTYK/CfdfHbBcl1HP7R2RQgYCUTOG/rksc35LtLgXfAgED
o1EwTzALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJ/PI
FR5umgIJFq0roIlgX9p7L6owEAYJKwYBBAGCNxUBBAMCAQAwDQYJKoZIhvcNAQEF
BQADggEBAJ2dhISjQal8dwy3U8pORFBi71R803UXHOjgxkhLtv5MOhmBVrBW7hmW
Yqpao2TB9k5UM8Z3/sUcuuVdJcr18JOagxEu5sv4dEX+5wW4q+ffy0vhN4TauYuX
cB7w4ovXsNgOnbFp1iqRe6lJT37mjpXYgyc81WhJDtSd9i7rp77rMKSsH0T8lasz
Bvt9YAretIpjsJyp8qS5UwGH0GikJ3+r/+n6yUA4iGe0OcaEb1fJU9u6ju7AQ7L4
CYNu/2bPPu8Xs1gYJQk0XuPL1hS27PKSb3TkL4Eq1ZKR4OCXPDJoBYVL0fdX4lId
kxpUnwVwwEpxYB5DC2Ae/qPOgRnhCzU=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEPDCCAySgAwIBAgIKYQlufQAAAAAADDANBgkqhkiG9w0BAQUFADA1MRYwFAYD
VQQKEw1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENBIDIwNDgw
HhcNMTEwNjMwMTc1NjU3WhcNMjkwNTE0MjAyNTQyWjAnMQ4wDAYDVQQKEwVDaXNj
bzEVMBMGA1UEAxMMQUNUMiBTVURJIENBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEA0m5l3THIxA9tN/hS5qR/6UZRpdd+9aE2JbFkNjht6gfHKd477AkS
5XAtUs5oxDYVt/zEbslZq3+LR6qrqKKQVu6JYvH05UYLBqCj38s76NLk53905Wzp
9pRcmRCPuX+a6tHF/qRuOiJ44mdeDYZo3qPCpxzprWJDPc1M4iYKHumMQMqmgmg+
xghHIooWS80BOcdiynEbeP5rZ7qRuewKMpl1TiI3WdBNjZjnpfjg66F+P4SaDkGb
BXdGj13oVeF+EyFWLrFjj97fL2+8oauV43Qrvnf3d/GfqXj7ew+z/sXlXtEOjSXJ
URsyMEj53Rdd9tJwHky8neapszS+r+kdVQIDAQABo4IBWjCCAVYwCwYDVR0PBAQD
AgHGMB0GA1UdDgQWBBRI2PHxwnDVW7t8cwmTr7i4MAP4fzAfBgNVHSMEGDAWgBQn
88gVHm6aAgkWrSugiWBf2nsvqjBDBgNVHR8EPDA6MDigNqA0hjJodHRwOi8vd3d3
LmNpc2NvLmNvbS9zZWN1cml0eS9wa2kvY3JsL2NyY2EyMDQ4LmNybDBQBggrBgEF
```

```
BQcBAQREMEIwQAYIKwYBBQUHMAKGNGh0dHA6Ly93d3cuY2lzY28uY29tL3NlY3Vy
aXR5L3BraS9jZXJ0cy9jcmNhMjA0OC5jZXIwXAYDVR0gBFUwUzBRBgorBgEEAQkV
AQwAMEMwQQYIKwYBBQUHAgEWNWh0dHA6Ly93d3cuY2lzY28uY29tL3NlY3VyaXR5
L3BraS9wb2xpY2llcy9pbmRleC5odG1sMBIGA1UdEwEB/wQIMAYBAf8CAQAwDQYJ
KoZIhvcNAQEFBQADggEBAGh1qclr9tx4hzWgDERm371yeuEmqcIfi9b9+GbMSJbi
ZHc/CcCl0lJu0a9zTXA9w47H9/t6leduGxb4WeLxcwCiUgvFtCa51Iklt8nNbcKY
/4dw1ex+7amATUQO4QggIE67wVIPu6bgAE3Ja/nRS3xKYSnj8H5TehimBSv6TECi
i5jUhOWryAK4dVo8hCjkjEkzu3ufBTJapnv89g9OE+H3VKM4L+/KdkUO+52djFKn
hyl47d7cZR4DY4LIuFM2P1As8YyjzoNpK/urSRI14WdIlplR1nH7KNDl5618yfVP
0IFJZBGrooCRBjOSwFv8cpWCbmWdPaCQT2nwIjTfY8c=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDhjCCAm6gAwIBAgIDctWkMA0GCSqGSIb3DQEBCwUAMCcxDjAMBgNVBAoTBUNp
c2NvMRUwEwYDVQQDEwxBQ1QyIFNVREkgQ0EwHhcNMTUwODA2MDgwODI5WhcNMjUw
ODA2MDgwODI5WjBzMSwwKgYDVQQFEyNQSUQ6V1MtQzM2NTAtMTJYNDhVWiBTTjpG
RE8xOTMyWDAwQzEOMAwGA1UEChMFQ2lzY28xGDAWBgNVBAsTD0FDVC0yIExpdGUg
U1VESTEZMBcGA1UEAxMQV1MtQzM2NTAtMTJYNDhVWjCCASIwDQYJKoZIhvcNAQEB
BQADggEPADCCAQoCggEBANZxOGYI0eUl4HcSwjL4HO75qTjl9C2BHG3ufce9ikkN
xwGXi8qg8vKxuB9tRYRaJC5bP1WMoq7+ZJtQA079xE4X14soNbkq5NaUhh7RB1wD
iRUJvTfCOzVICbNfbzvtB30I75tCarFNmpd0K6AFrIa41U988QGqaCj7R1JrYNaj
nC73UXXM/hC0HtNR5mhyqer5Y2qjjzo6tHZYqrrx2eS1XOa262ZSQriAxmaH/KLC
K97ywyRBdJlxBRX3hGtKlog8nASB8WpXqB9NVCERzUajwU3L/kg2BsCqw9Y2m7HW
U1cerTxgthuyUkdNI+Jg6iGApm2+s8E9hsHPBPMCdIsCAwEAAaNvMG0wDgYDVR0P
AQH/BAQDAgXgMAwGA1UdEwEB/wQCMAAwTQYDVR0RBEYwRKBCBgkrBgEEAQkVAgOg
NRMzQ2hpcElEPVVZSk5ORmRRRlFvN1ZIVmxJRTlqZENBeU9DQXhPRG93TlRveE1T
QVg5eWc9MA0GCSqGSIb3DQEBCwUAA4IBAQBKicTRZbVCRjVIR5MQcWXUT086v6Ej
HahDHTts3YpQoyAVfioNg2x8J6EXcEau4voyVu+eMUuoNL4szPhmmDcULfiCGBcA
/R3EFuoVMIzNT0geziytsCf728KGw1oGuosgVjNGOOahUELu4+F/My7bIJNbH+PD
KjIFmhJpJg0F3q17yClAeXvd13g3W393i35d00Lm5L1WbBfQtyBaOLAbxsHvutrX
u1VZ5sdqSTwTkkO9vKMaQjh7a8J/AmJi93jvzM69pe5711P1zqZfYfpiJ3cyJ0xf
I4brQ1smdczloFD4asF7A+1vor5e4VDBP0ppmeFAJvCQ52JTpj0M0o1D
-----END CERTIFICATE-----
```

show running-config

To display the contents of the current running configuration file or the configuration for a specific module, Layer 2 VLAN, class map, interface, map class, policy map, or virtual circuit (VC) class, use the **show running-config** command in privileged EXEC mode.

show running-config [*options*]

Syntax Description

options (Optional) Keywords used to customize output. You can enter more than one keyword.

- **aaa** [**accounting** | **attribute** | **authentication** | **authorization** | **diameter** | **group** | **ldap** | **miscellaneous** | **radius-server** | **server** | **tacacs-server** | **user-name** | **username**]: Displays AAA configurations.
- **all**: Expands the output to include the commands that are configured with default parameters. If the **all** keyword is not used, the output does not display commands configured with default parameters.
- **bridge-domain** {**id** | **parameterized vlan**}: Displays the running configuration for bridge domains.
- **brief**: Displays the configuration without certification data and encrypted filter details.
- **class-map** [*name*] [**linenum**]: Displays class map information.
- **cts** [**interface** | **policy-server** | **rbm-rbac** | **server** | **sxp**] : Displays Cisco TrustSec configurations.
- **deprecated**: Displays deprecated configuration along with the running configuration.
- **eap** {**method** | **profiles**}: Displays EAP method configurations and profiles.
- **flow** {**exporter** | **monitor** | **record**}: Displays global flow configuration commands.
- **full**: Displays the full configuration.
- **identity** {**policy** | **profile**}: Displays identity profile or policy information.

- **interface** *type number*: Displays interface-specific configuration information. If you use the **interface** keyword, you must specify the interface type and the interface number (for example, **interface GigabitEthernet 1/0/1**). Use the **show run interface ?** command to determine the interfaces available on your system.
- **ip dhcp pool** [*name*]: Displays IPv4 DHCP pool configuration.
- **ipv6 dhcp pool** [*name*]: Displays IPv6 DHCP pool configuration.
- **linenum** [**brief** | **full** | **partition**]: Displays line numbers in the output.
- **map-class** [**atm** | **dialer** | **frame-relay**] [*name*]: Displays map class information.
- **mdns-sd** [**gateway** | **location-group** | **service-definition** | **service-list** | **service-peer** | **service-policy**]: Displays Multicast DNS Service Discovery (mDNS-SD) configurations.
- **partition** {**access-list** | **class-map** | **common** | **global-cdp** | **interface** | **ip-as-path** | **ip-community** | **ip-prefix-list** | **ip-static-routes** | **line** | **policy-map** | **route-map** | **router** | **snmp** | **tacacs**}: Displays the configuration corresponding to a partition.
- **policy-map** [*name*] [**linenum**]: Displays policy map information.
- **switch** *number*: Displays configuration for the specified switch.
- **view** [**full**]: Enables the display of a full running configuration. This is for view-based users who typically can only view the configuration commands that they are entitled to access for that particular view.
- **vlan** [*vlan-id*]: Displays the specific VLAN information; valid values are from 1 to 4094.
- **vrf** [*vrf-name*]: Displays the Virtual routing and forwarding (VRF)-aware configuration module number .

Command Default

The default syntax, **show running-config**, displays the contents of the running configuration file, except commands configured using the default parameters.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The **show running-config** command is technically a command alias (substitute or replacement syntax) of the **more system:running-config** command. Although the use of more commands is recommended (because of their uniform structure across platforms and their expandable syntax), the **show running-config** command remains enabled to accommodate its widespread use, and to allow typing shortcuts such as **show run**.

The **show running-config interface** command is useful when there are multiple interfaces and you want to look at the configuration of a specific interface.

The **linenum** keyword causes line numbers to be displayed in the output. This option is useful for identifying a particular portion of a very large configuration.

You can enter additional output modifiers in the command syntax by including a pipe character (|) after the optional keyword. For example, **show running-config interface GigabitEthernet 1/0/1 linenum | begin 3**.

To display the output modifiers that are available for a keyword, enter **| ?** after the keyword. Depending on the platform you are using, the keywords and the arguments for the *options* argument may vary.

The **show running-config all** command displays complete configuration information, including the default settings and values. For example, if the Cisco Discovery Protocol (abbreviated as CDP in the output) hold-time value is set to its default of 180:

- The **show running-config** command does not display this value.
- The **show running-config all** displays the following output: cdp holdtime 180.

If the Cisco Discovery Protocol holdtime is changed to a nondefault value (for example, 100), the output of the **show running-config** and **show running-config all** commands is the same; that is, the configured parameter is displayed.

The **show running-config** command displays ACL information. To exclude ACL information from the output, use the **show running | section exclude ip access | access list** command.

Examples

The following example shows the configuration for GigabitEthernet0/0 interface. The fields are self-explanatory.

```
Device# show running-config interface gigabitEthernet0/0

Building configuration...

Current configuration : 130 bytes
!
interface GigabitEthernet0/0
 vrf forwarding Mgmt-vrf
 ip address 10.5.20.10 255.255.0.0
 negotiation auto
 ntp broadcast
end
```

The following example shows how to set line numbers in the command output and then use the output modifier to start the display at line 10. The fields are self-explanatory.

```
Device# show running-config linenum | begin 10

   10 : boot-start-marker
   11 : boot-end-marker
   12 : !
   13 : no logging buffered
   14 : enable password #####
   15 : !
   16 : spe 1/0 1/7
   17 :  firmware location bootflash:mica-modem-pw.10.16.0.0.bin
   18 : !
   19 : !
   20 : resource-pool disable
   21 : !
   22 : no aaa new-model
   23 : ip subnet-zero
   24 : ip domain name cisco.com
   25 : ip name-server 172.16.11.48
   26 : ip name-server 172.16.2.133
   27 : !
   28 : !
   29 : isdn switch-type primary-5ess
   30 : !
   .
```

```
.
.
126 : end
```

In the following sample output from the **show running-config** command, the **shape average** command indicates that the traffic shaping overhead accounting for ATM is enabled. The BRAS-DSLAM encapsulation type is qinq and the subscriber line encapsulation type is snap-rbe based on the ATM adaptation layer 5 (AAL5) service. The fields are self-explanatory.

```
Device# show running-config
.
.
.
subscriber policy recording rules limit 64
no mpls traffic-eng auto-bw timers frequency 0
call rsvp-sync
!
controller T1 2/0
framing sf
linecode ami
!
controller T1 2/1
framing sf
linecode ami
!
!
policy-map unit-test
class class-default
shape average percent 10 account qinq aal5 snap-rbe
!
```

The following is sample output from the **show running-config class-map** command. The fields in the display are self-explanatory.

```
Device# show running-config class-map

Building configuration...

Current configuration : 2157 bytes
!
class-map match-any system-cpp-police-ewlc-control
  description EWLC Control
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 packets, LOGGING, Transit Traffic
class-map match-any system-cpp-default
  description EWLC Data, Inter FED Traffic
class-map match-any system-cpp-police-sys-data
  description Openflow, Exception, EGR Exception, NFL Sampled Data, RPF Failed
class-map match-any system-cpp-police-punt-webauth
  description Punt Webauth
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-high-rate-app
  description High Rate Applications
class-map match-any system-cpp-police-multicast
  description 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 OOB
...
```

The following example shows that the teletype (tty) line 2 is reserved for communicating with the second core:

```
Device# show running

Building configuration...

Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname device
!
enable password lab
!
no ip subnet-zero
!
!
!
interface Ethernet0
 ip address 10.25.213.150 255.255.255.128
 no ip directed-broadcast
 no logging event link-status
!
interface Serial0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 shutdown
 no fair-queue
!
interface Serial1
 no ip address
 no ip directed-broadcast
 shutdown
!
ip default-gateway 10.25.213.129
ip classless
ip route 0.0.0.0 0.0.0.0 10.25.213.129
!
!
line con 0
 transport input none
line 1 6
 no exec
 transport input all
line 7
 no exec
 exec-timeout 300 0
 transport input all
line 8 9
 no exec
 transport input all
```

```
line 10
 no exec
 transport input all
 stopbits 1
line 11 12
 no exec
 transport input all
line 13
 no exec
 transport input all
 speed 115200
line 14 16
 no exec
 transport input all
line aux 0
line vty 0 4
 password cisco
 login
!
end
```

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration. (Command alias for the **copy system:running-config nvram:startup-config** command.)
show startup-config	Displays the contents of NVRAM (if present and valid) or displays the configuration file pointed to by the CONFIG_FILE environment variable. (Command alias for the **more:nvram startup-config** command.)

show sdm prefer

To display information about the templates that can be used to maximize system resources for a particular feature, use the **show sdm prefer** command in privileged EXEC mode. To display the current template, use the command without a keyword.

show sdm prefer [**advanced**]

Syntax Description

advanced	(Optional) Displays information on the advanced template.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

If you did not reload the switch after entering the **sdm prefer** global configuration command, the **show sdm prefer** privileged EXEC command displays the template currently in use and not the newly configured template.

The numbers displayed for each template represent an approximate maximum number for each feature resource. The actual number might vary, depending on the actual number of other features configured. For example, in the default template if your 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:

```
# show sdm prefer

Showing SDM Template Info

This is the Advanced template.
 Number of VLANs:                                4094
 Unicast MAC addresses:                          32768
 Overflow Unicast MAC addresses:                 512
 IGMP and Multicast groups:                      8192
 Overflow IGMP and Multicast groups:             512
 Directly connected routes:                      32768
 Indirect routes:                                7680
 Security Access Control Entries:                3072
 QoS Access Control Entries:                     3072
 Policy Based Routing ACEs:                      1024
 Netflow ACEs:                                   1024
 Input Microflow policer ACEs:                   256
 Output Microflow policer ACEs:                  256
 Flow SPAN ACEs:                                 256
 Tunnels:                                        256
```

```
 Control Plane Entries:                          512
 Input Netflow flows:                           8192
 Output Netflow flows:                         16384
 SGT/DGT entries:                               4096
 SGT/DGT Overflow entries:                       512
These numbers are typical for L2 and IPv4 features.
Some features such as IPv6, use up double the entry size;
so only half as many entries can be created.

#
```

show tech-support license

To display the debug output, use the **show license tech support** command in privileged EXEC mode.

show tech-support license

Syntax Description

This command has no arguments or keywords.

Command Default

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.1	This command was introduced.

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

Command	Description
show license all	Displays entitlements information.
show license status	Displays compliance status of a license.

Command	Description
show license summary	Displays summary of all active licenses.
show license udi	Displays UDI.
show license usage	Displays license usage information

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.

show tech-support platform

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

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
```

```
 IHQ: pkts in input hold queue     IQD: pkts dropped from input queue
 OHQ: pkts in output hold queue    OQD: pkts dropped from output queue
 RXBS: rx rate (bits/sec)          RXPS: rx rate (pkts/sec)
 TXBS: tx rate (bits/sec)          TXPS: tx rate (pkts/sec)
 TRTL: throttle count

  Interface                   IHQ       IQD       OHQ       OQD       RXBS       RXPS
TXBS      TXPS      TRTL
------------------------------------------------------------------------------------------------------------------

  Vlan1                         0         0         0         0          0          0
  0         0         0
* GigabitEthernet0/0            0     10179         0         0       2000          4
  0         0         0
  GigabitEthernet1/0/1          0         0         0         0          0          0
  0         0         0
  GigabitEthernet1/0/2          0         0         0         0          0          0
  0         0         0
  GigabitEthernet1/0/3          0         0         0         0          0          0
  0         0         0
  GigabitEthernet1/0/4          0         0         0         0          0          0
  0         0         0
  GigabitEthernet1/0/5          0         0         0         0          0          0
  0         0         0
  GigabitEthernet1/0/6          0         0         0         0          0          0
  0         0         0
  GigabitEthernet1/0/7          0         0         0         0          0          0
  0         0         0
  GigabitEthernet1/0/8          0         0         0         0          0          0
  0         0         0
  GigabitEthernet1/0/9          0         0         0         0          0          0
  0         0         0
  GigabitEthernet1/0/10         0         0         0         0          0          0
  0         0         0
  GigabitEthernet1/0/11         0         0         0         0          0          0
  0         0         0
  GigabitEthernet1/0/12         0         0         0         0          0          0
  0         0         0
  GigabitEthernet1/0/13         0         0         0         0          0          0
  0         0         0
  GigabitEthernet1/0/14         0         0         0         0          0          0
  0         0         0
  GigabitEthernet1/0/15         0         0         0         0          0          0
  0         0         0
  GigabitEthernet1/0/16         0         0         0         0          0          0
  0         0         0
  GigabitEthernet1/0/17         0         0         0         0          0          0
  0         0         0
  GigabitEthernet1/0/18         0         0         0         0          0          0
  0         0         0
  GigabitEthernet1/0/19         0         0         0         0          0          0
  0         0         0
  GigabitEthernet1/0/20         0         0         0         0          0          0
  0         0         0
  GigabitEthernet1/0/21         0         0         0         0          0          0
  0         0         0
  GigabitEthernet1/0/22         0         0         0         0          0          0
  0         0         0
  GigabitEthernet1/0/23         0         0         0         0          0          0
  0         0         0
  GigabitEthernet1/0/24         0         0         0         0          0          0
  0         0         0
  GigabitEthernet1/0/25         0         0         0         0          0          0
  0         0         0
```

```
  GigabitEthernet1/0/26          0          0          0          0          0          0
  0          0          0
  GigabitEthernet1/0/27          0          0          0          0          0          0
  0          0          0
  GigabitEthernet1/0/28          0          0          0          0          0          0
  0          0          0
  GigabitEthernet1/0/29          0          0          0          0          0          0
  0          0          0
  GigabitEthernet1/0/30          0          0          0          0          0          0
  0          0          0
  GigabitEthernet1/0/31          0          0          0          0          0          0
  0          0          0
  GigabitEthernet1/0/32          0          0          0          0          0          0
  0          0          0
  GigabitEthernet1/0/33          0          0          0          0          0          0
  0          0          0
  GigabitEthernet1/0/34          0          0          0          0          0          0
  0          0          0
  GigabitEthernet1/0/35          0          0          0          0          0          0
  0          0          0
  GigabitEthernet1/0/36          0          0          0          0          0          0
  0          0          0
  Te1/0/37                       0          0          0          0          0          0
  0          0          0
  Te1/0/38                       0          0          0          0          0          0
  0          0          0
  Te1/0/39                       0          0          0          0          0          0
  0          0          0
  Te1/0/40                       0          0          0          0          0          0
  0          0          0
  Te1/0/41                       0          0          0          0          0          0
  0          0          0
  Te1/0/42                       0          0          0          0          0          0
  0          0          0
  Te1/0/43                       0          0          0          0          0          0
  0          0          0
  Te1/0/44                       0          0          0          0          0          0
  0          0          0
  Te1/0/45                       0          0          0          0          0          0
  0          0          0
  Te1/0/46                       0          0          0          0          0          0
  0          0          0
  Te1/0/47                       0          0          0          0          0          0
  0          0          0
  Te1/0/48                       0          0          0          0          0          0
  0          0          0
  Te1/1/1                        0          0          0          0          0          0
  0          0          0
  Te1/1/2                        0          0          0          0          0          0
  0          0          0
  Te1/1/3                        0          0          0          0          0          0
  0          0          0
  Te1/1/4                        0          0          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.

Related Commands

Command	Description
show tech-support platform evpn_vxlan	Displays EVPN-VXLAN-related platform information.
show tech-support platform fabric	Displays detailed information about the switch fabic.
show tech-support platform igmp_snooping	Displays IGMP snooping information about a group.
show tech-support platform layer3	Displays Layer 3 platform forwarding information.
show tech-support platform mld_snooping	Displays MLD snooping information about a group.

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

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

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 sdm 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
  MVPN MDT Tunnels:                                     256
  L2 VPN EOMPLS Attachment Circuit:                     256
  MAX VPLS Bridge Domains :                             64
  MAX VPLS Peers Per Bridge Domain:                     8
  MAX VPLS/VPWS 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
 0x4  MAT_DISCARD_ADDR           0x8
MAT_ALL_VLANS             0x10  MAT_NO_FORWARD            0x20  MAT_IPMULT_ADDR
0x40  MAT_RESYNC                0x80
MAT_DO_NOT_AGE           0x100  MAT_SECURE_ADDR          0x200  MAT_NO_PORT
0x400  MAT_DROP_ADDR            0x800
MAT_DUP_ADDR            0x1000  MAT_NULL_DESTINATION    0x2000  MAT_DOT1X_ADDR
0x4000  MAT_ROUTER_ADDR         0x8000
MAT_WIRELESS_ADDR      0x10000  MAT_SECURE_CFG_ADDR    0x20000  MAT_OPQ_DATA_PRESENT
0x40000  MAT_WIRED_TUNNEL_ADDR  0x80000
MAT_DLR_ADDR          0x100000  MAT_MRP_ADDR          0x200000  MAT_MSRP_ADDR
0x400000  MAT_LISP_LOCAL_ADDR   0x800000
MAT_LISP_REMOTE_ADDR 0x1000000  MAT_VPLS_ADDR        0x2000000
Device#
```

Output fields are self-explanatory.

Related Commands

Command	Description
show tech-support platform	Displays detailed information about a platform for use by technical support.

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

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

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 10.1.1.1/32 dest instance-id 4098 ipv4 10.12.12.12/32

.
.
.
-----show ip lisp eid-table vrf DEFAULT_VN forwarding  eid remote 10.12.12.12-----


Prefix                 Fwd action  Locator status bits   encap_iid
10.12.12.12/32         encap       0x00000001            N/A
  packets/bytes       1/576
  path list 7F44EEC2C188, 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 LISP0.4098, IP midchain out of LISP0.4098, addr 192.0.2.2
7F44F8E86CE8
    1 output chain
      chain[0]: IP midchain out of LISP0.4098, addr 192.0.2.2 7F44F8E86CE8
                IP adj out of GigabitEthernet1/0/1, addr 10.0.2.1 7F44F8E87378


-----show lisp instance-id 4098 ipv4 map-cache-----


LISP IPv4 Mapping Cache for EID-table vrf DEFAULT_VN (IID 4098), 3 entries

0.0.0.0/0, uptime: 02:46:01, expires: never, via static-send-map-request
  Encapsulating to proxy ETR
10.1.1.0/24, uptime: 02:46:01, expires: never, via dynamic-EID, send-map-request
  Encapsulating to proxy ETR
10.12.12.12/32, uptime: 02:45:54, expires: 21:14:06, via map-reply, complete
  Locator  Uptime    State      Pri/Wgt     Encap-IID
  192.0.2.2  02:45:54  up          10/10        -


-----show lisp instance-id 4098 ipv4  map-cache detail-----


LISP IPv4 Mapping Cache for EID-table vrf DEFAULT_VN (IID 4098), 3 entries

0.0.0.0/0, uptime: 02:46:01, expires: never, via static-send-map-request
  Sources: static-send-map-request
  State: send-map-request, last modified: 02:46:01, map-source: local
  Exempt, Packets out: 2(676 bytes) (~ 02:45:38 ago)
  Configured as EID address space
  Encapsulating to proxy ETR
101.1.0/24, uptime: 02:46:01, expires: never, via dynamic-EID, send-map-request
  Sources: NONE
  State: send-map-request, last modified: 02:46:01, map-source: local
  Exempt, Packets out: 0(0 bytes)
  Configured as EID address space
  Configured as dynamic-EID address space
  Encapsulating dynamic-EID traffic
  Encapsulating to proxy ETR
```

```
10.12.12.12/32, uptime: 02:45:54, expires: 21:14:06, via map-reply, complete
  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

10.12.12.12/32, uptime: 02:45:54, expires: 21:14:06, via map-reply, complete
  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 7F44EEC2C188, 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 LISP0.4098, IP midchain out of LISP0.4098, addr 192.0.2.2
7F44F8E86CE8
        1 output chain
          chain[0]: IP midchain out of LISP0.4098, 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:
    LISP0.4098(78): 192.0.2.2
  path list 7F44EEC2C188, 3 locks, per-destination, flags 0x49 [shble, rif, hwcn]
    path 7F44F8B5AFF0, share 10/10, type attached nexthop, for IPv4
     nexthop 192.0.2.2 LISP0.4098, IP midchain out of LISP0.4098, addr 192.0.2.2 7F44F8E86CE8

  output chain:
    PushCounter(LISP:10.12.12.12/32) 7F44F3C8B8D8
    IP midchain out of LISP0.4098, 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.

Related Commands

Command	Description
show tech-support platform	Displays detailed information about a platform for use by technical support.

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

Group_ipAddr	(Optional) Displays snooping information about the specified group address.
ipv4-address	(Optional) IPv4 address of the group.
vlan *vlan-ID*	(Optional) Displays IGMP snooping VLAN information. Valid values are from 1 to 4094.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

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
```

```
  25    Router


----- show ip igmp snooping querier -----


Vlan      IP Address              IGMP Version   Port
-----------------------------------------------------------
23        10.1.1.1                v2             Router
24        10.1.2.1                v2             Router
25        10.1.3.1                v2             Router


----- 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-dvmrp
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 -----

Vlan      Group                   Type        Version     Port List
------------------------------------------------------------------------------
5         226.6.6.6               user                    Gi1/0/8, Gi1/0/27, Gi1/0/28,
                                                          Gi2/0/7, Gi2/0/8, Gi2/0/27,
                                                          Gi2/0/28
5         238.192.0.1             user                    Gi2/0/28


----- show platform software fed active ip igmp snooping vlan 5 -----


Vlan 5
---------
 IGMPSN Enabled  : On
 PIMSN Enabled   : Off
 Flood Mode      : On
 I-Mrouter       : Off
 Oper State      : Up
```

```
 STP TCN Flood   : Off
 Routing Enabled : Off
 PIM Enabled     : Off
 PVLAN           : No
 In Retry        : 0x0
 L3mcast Adj      :
 Mrouter PortQ   :
 Flood PortQ     :


----- show platform software fed active ip igmp snooping groups | begin 226.6.6.6 -----

Vlan:5 Group:226.6.6.6
--------------------------------
Member ports   :
CAPWAP ports   :
Host Type Flags: 0
Failure Flags  : 0
DI handle      : 0x7f11151cbad8
REP RI handle  : 0x7f11151cc018
SI handle      : 0x7f11151cd198
HTM handle     : 0x7f11151cd518

si hdl : 0x7f11151cd198 rep ri hdl : 0x7f11151cc018 di hdl :  0x7f11151cbad8 htm hdl :
0x7f11151cd518
.
.
.
Device#
```

Output fields are self-explanatory.

Related Commands

Command	Description
ip igmp snooping	Enables IGMP snooping globally or on an interface.
show ip igmp snooping	Displays the IGMP snooping configuration of a device.
show tech-support platform	Displays detailed information about a platform for use by technical support.

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

multicast	Displays multicast information.
Group_ipv6Addr *ipv4-address*	Displays information about the specified multicast group address.
switch *switch-number*	Displays information about the specified switch. Valid values are from 1 to 9.
srcIP *ipv4-address*	Displays information about the specified source address.
unicast	Displays unicast-related information.
dstIP *ipv4-address*	Displays information about the specified destination address.
vrf *vrf-name*	Displays unicast-related virtual routing and forwarding (VRF) information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

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 -----


IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       G - Received BGP C-Mroute, g - Sent BGP C-Mroute,
       N - Received BGP Shared-Tree Prune, n - BGP C-Mroute suppressed,
       Q - Received BGP S-A Route, q - Sent BGP S-A Route,
       V - RD & Vector, v - Vector, p - PIM Joins on route,
       x - VxLAN group, c - PFP-SA cache created entry
Outgoing interface flags: H - Hardware switched, A - Assert winner, p - PIM Join
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode

(10.10.0.2, 224.1.1.1), 00:00:22/00:02:37, flags: LFT
  Incoming interface: GigabitEthernet1/0/10, RPF nbr 0.0.0.0, Registering
  Outgoing interface list:
    Vlan20, Forward/Sparse, 00:00:22/00:02:37, A



----- show ip mfib 224.1.1.1 10.10.0.2 -----


Entry Flags:    C - Directly Connected, S - Signal, IA - Inherit A flag,
                ET - Data Rate Exceeds Threshold, K - Keepalive
                DDE - Data Driven Event, HW - Hardware Installed
                ME - MoFRR ECMP entry, MNE - MoFRR Non-ECMP entry, MP - MFIB
                MoFRR Primary, RP - MRIB MoFRR Primary, P - MoFRR Primary
                MS  - MoFRR  Entry in Sync, MC - MoFRR entry in MoFRR Client.
I/O Item Flags: IC - Internal Copy, NP - Not platform switched,
                NS - Negate Signalling, SP - Signal Present,
                A - Accept, F - Forward, RA - MRIB Accept, RF - MRIB Forward,
                MA - MFIB Accept, A2 - Accept backup,
                RA2 - MRIB Accept backup, MA2 - MFIB Accept backup

Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts:      Total/RPF failed/Other drops
I/O Item Counts:   FS Pkt Count/PS Pkt Count
Default
 (10.10.0.2,224.1.1.1) Flags: HW
   SW Forwarding: 0/0/0/0, Other: 1/1/0
   HW Forwarding:   NA/NA/NA/NA, Other: NA/NA/NA
   GigabitEthernet1/0/10 Flags: A
   Vlan20 Flags: F IC
     Pkts: 0/0
   Tunnel0 Flags: F
     Pkts: 0/0



----- show platform software fed switch 1 ip multicast interface summary -----

Multicast Interface database
```

```
VRF  Interface                IF ID              PIM Status  State              RI Handle
           SVI
-------------------------------------------------------------------------------------------------------
0    GigabitEthernet1/0/10     0x000000000000005f  enabled     0x0000000000000010
0x00007fb414b1f108  false
0    Vlan20                    0x0000000000000060  enabled     0x0000000000000010
0x00007fb414b31a98  true



----- 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: 0x00007fb414b2b678  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 -----


MROUTE ENTRY vrf 0 (10.10.0.2, 224.1.1.1/32)
  HW Handle: 140411418055080 Flags:  IC
RPF interface: GigabitEthernet1/0/10(95)):
  HW Handle:140411418055080 Flags:A
Number of OIF: 3
Flags: 0x4   Pkts : 0
OIF Details:
     Tunnel0      Adj: 0xf8000636    F
     Vlan20      Adj: 0xf8000601  F IC
     GigabitEthernet1/0/10        A
Htm: 0x7fb414b2f348  Si: 0x7fb414b321d8  Di: 0x7fb414b2dba8  Rep_ri: 0x7fb414b30ed8


DI details
----------
Handle:0x7fb414b2dba8 Res-Type:ASIC_RSC_DI Res-Switch-Num:255 Asic-Num:255
Feature-ID:AL_FID_L3_
MULTICAST_IPV4 Lkp-ftr-id:LKP_FEAT_INVALID ref_count:1
priv_ri/priv_si Handle:(nil) Hardware Indices/Handles: index0:0x538e
mtu_index/l3u_ri_index0:0x0  index1:0x538e  mtu_index/l3u_ri_index1:0x0
```

```
Cookie length: 56
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
Detailed Resource Information (ASIC# 0)
----------------------------------------

Destination Index (DI) [0x538e]
portMap = 0x00000000                0
cmi1 = 0x385
rcpPortMap = 0

al_rsc_cmi
CPU Map Index (CMI) [0x385]
ctiLo0 = 0x9
ctiLo1 = 0
ctiLo2 = 0
cpuQNum0 = 0x9e
cpuQNum1 = 0
cpuQNum2 = 0
npuIndex = 0
strip_seg = 0x0
copy_seg = 0x0
Detailed Resource Information (ASIC# 1)
----------------------------------------

Destination Index (DI) [0x538e]
portMap = 0x00000000                0
cmi1 = 0x385
rcpPortMap = 0

al_rsc_cmi
CPU Map Index (CMI) [0x385]
ctiLo0 = 0x9
ctiLo1 = 0
ctiLo2 = 0
cpuQNum0 = 0x9e
cpuQNum1 = 0
cpuQNum2 = 0
npuIndex = 0
strip_seg = 0x0
copy_seg = 0x0

============================================================

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_ri/priv_si Handle:(nil) Hardware Indices/Handles: 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 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
Detailed Resource Information (ASIC# 0)
----------------------------------------

Detailed Resource Information (ASIC# 1)
----------------------------------------


============================================================
```

```
SI details
----------
Handle:0x7fb414b321d8 Res-Type:ASIC_RSC_SI_STATS Res-Switch-Num:255 Asic-Num:255 Feature-ID:
AL_FID_L3_MULTICAST_IPV4 Lkp-ftr-id:LKP_FEAT_INVALID ref_count:1
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 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
                                             H/W   Current
Switch#   Role    Mac Address     Priority Version  State
------------------------------------------------------------------------------------------
*1       Active   5006.ab89.0280     1      V02     Ready




----- show switch -------
```

```
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 -----


nexthop is 10.0.0.20


Protocol Interface                 Address
IP       GigabitEthernet1/0/7      10.0.0.20(8)
                                   0 packets, 0 bytes
                                   epoch 0
                                   sourced in sev-epoch 0
                                   Encap length 14
                                   00211BFDE6495006AB8902C00800
                                   L2 destination address byte offset 0
                                   L2 destination address byte length 6
                                   Link-type after encap: ip
                                   ARP


----- 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 -----
```

```
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: 0:21:1b:fd:e6:49:50:6:ab:89:2:c0:8:0
  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: 0:21:1b:fd:e6:49:50:6:ab:89:2:c0:8:0
  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.

Related Commands

Command	Description
show tech-support platform	Displays detailed information about a platform for use by technical support.

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

Group_ipv6Addr	(Optional) Displays snooping information about the specified group address.
ipv6-address	(Optional) IPv6 address of the group.
vlan *vlan-ID*	(Optional) Displays MLD snooping VLAN information. Valid values are from 1 to 4094.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

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 300D0609 2A864886 F70D0101 05050030
  30312E30 2C060355 04031325 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 35353934 33333336 38301E17 0D313531 32303331 32353432
  325A170D 32303031 30313030 30303030 5A303031 2E302C06 03550403 1325494F
  532D5365 6C662D53 69676E65 642D4365 72746966 69636174 652D3535 39343333
  33363830 819F300D 06092A86 4886F70D 01010105 0003818D 00308189 02818100
  AD8C9C3B FEE7FFC8 986837D2 4C126172 446C3C53 E040F798 4BA61C97 7506FDCE
  46365D0A E47E3F4F C774CA5B 73E2A8DD B72A2E98 C66DB196 94E8150F 0B669CF6
  AA5BC4CD FC2E02F6 FE08B17F 0164FC19 7DC84ABB C99D91D6 398233FF 814EF6DA
  6DC8FC20 CA12C0D6 1CB28EDA 6ADD6DFA 7E3E8281 4A189A9A AA44FCC0 BA9BD8A5
  02030100 01A35330 51300F06 03551D13 0101FF04 05300301 01FF301F 0603551D
```

```
  23041830 16801448 668D668E C92914BB 69E9BA64 F61228DE 132E2030 1D060355
  1D0E0416 04144866 8D668EC9 2914BB69 E9BA64F6 1228DE13 2E20300D 06092A86
  4886F70D 01010505 00038181 0000F1D3 3DD1E5F1 EB714A95 D5819933 CAD0C943
  59927D55 9D70CAD0 D64830EB D54380AD D2B5B613 F8AF7A5B 1F801134 246F760D
  5E5515DB D098304F 5086F6CE 88E8B576 F6B93A88 F458FDCF 91A42D7E FA741908
  5C892D78 600FB655 E6C5A4D0 6C1F1B9A 3AECA550 E3DC0881 01C4D004 7AB65BC3
  88CF24DE DAA19474 51B535A5 0C
   quit
crypto pki certificate chain SLA-TrustPoint
 certificate ca 01
  30820321 30820209 A0030201 02020101 300D0609 2A864886 F70D0101 0B050030
  32310E30 0C060355 040A1305 43697363 6F312030 1E060355 04031317 43697363
  6F204C69 63656E73 696E6720 526F6F74 20434130 1E170D31 33303533 30313934
  3834375A 170D3338 30353330 31393438 34375A30 32310E30 0C060355 040A1305
  43697363 6F312030 1E060355 04031317 43697363 6F204C69 63656E73 696E6720
  526F6F74 20434130 82012230 0D06092A 864886F7 0D010101 05000382 010F0030
  82010A02 82010100 A6BCBD96 131E05F7 145EA72C 2CD686E6 17222EA1 F1EFF64D
  CBB4C798 212AA147 C655D8D7 9471380D 8711441E 1AAF071A 9CAE6388 8A38E520
  1C394D78 462EF239 C659F715 B98C0A59 5BBB5CBD 0CFEBEA3 700A8BF7 D8F256EE
  4AA4E80D DB6FD1C9 60B1FD18 FFC69C96 6FA68957 A2617DE7 104FDC5F EA2956AC
  7390A3EB 2B5436AD C847A2C5 DAB553EB 69A9A535 58E9F3E3 C0BD23CF 58BD7188
  68E69491 20F320E7 948E71D7 AE3BCC84 F10684C7 4BC8E00F 539BA42B 42C68BB7
  C7479096 B4CB2D62 EA2F505D C7B062A4 6811D95B E8250FC4 5D5D5FB8 8F27D191
  C55F0D76 61F9A4CD 3D992327 A8BB03BD 4E6D7069 7CBADF8B DF5F4368 95135E44
  DFC7C6CF 04DD7FD1 02030100 01A34230 40300E06 03551D0F 0101FF04 04030201
  06300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604 1449DC85
  4B3D31E5 1B3E6A17 606AF333 3D3B4C73 E8300D06 092A8648 86F70D01 010B0500
  03820101 00507F24 D3932A66 86025D9F E838AE5C 6D4DF6B0 49631C78 240DA905
  604EDCDE FF4FED2B 77FC460E CD636FDB DD44681E 3A5673AB 9093D3B1 6C9E3D8B
  D98987BF E40CBD9E 1AECA0C2 2189BB5C 8FA85686 CD98B646 5575B146 8DFC66A8
  467A3DF4 4D565700 6ADF0F0D CF835015 3C04FF7C 21E878AC 11BA9CD2 55A9232C
  7CA7B7E6 C1AF74F6 152E99B7 B1FCF9BB E973DE7F 5BDDEB86 C71E3B49 1765308B
  5FB0DA06 B92AFE7F 494E8A9E 07B85737 F3A58BE1 1A48A229 C37C1E69 39F08678
  80DDCD16 D6BACECA EEBC7CF9 8428787B 35202CDC 60E4616A B623CDBD 230E3AFB
  418616A9 4093E049 4D10AB75 27E86F73 932E35B5 8862FDAE 0275156F 719BB2F0
  D697DF7F 28
   quit
!
!
!
diagnostic bootup level minimal
diagnostic monitor syslog
!
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 EWLC control, EWLC data, Inter FED
class-map match-any system-cpp-police-sys-data
  description Learning cache ovfl, High Rate App, Exception, EGR Exception, NFL SAMPLED
```

```
DATA, RPF Failed
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
!
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 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
!
!
!
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 -----

Vlan      Group                   Type        Version     Port List
-----------------------------------------------------------------------------
123       FF02::5:1               mld         v2          Gi2/0/1

Device#
```

Output fields are self-explanatory.

Related Commands

Command	Description
ipv6 mld snooping	Enables MLDv2 protocol snooping globally.
show ipv6 mld snooping	Displays MLDv2 snooping information.
show tech-support platform	Displays detailed information about a platform for use by technical support.

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

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

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**

- **show platform software fed switch ifm mappings gpn**
- **show platform software fed switch ifm mappings port-le**
- **show platform software fed switch ifm if-id**
- **show platform software fed switch active port if_id**

Examples

The following is sample output from the **show tech-support port** command:

```
Device# show tech-support port
.
.
.
  ----- show controllers utilization -----

Port       Receive Utilization  Transmit Utilization
Gi1/0/1       0   0
Gi1/0/2       0   0
Gi1/0/3       0   0
Gi1/0/4       0   0
Gi1/0/5       0   0
Gi1/0/6       0   0
Gi1/0/7       0   0
Gi1/0/8       0   0
Gi1/0/9       0   0
Gi1/0/10       0   0
Gi1/0/11       0   0
Gi1/0/12       0   0
Gi1/0/13       0   0
Gi1/0/14       0   0
Gi1/0/15       0   0
Gi1/0/16       0   0
Gi1/0/17       0   0
Gi1/0/18       0   0
Gi1/0/19       0   0
Gi1/0/20       0   0
Gi1/0/21       0   0
Gi1/0/22       0   0
Gi1/0/23       0   0
Gi1/0/24       0   0
Gi1/0/25       0   0
Gi1/0/26       0   0
Gi1/0/27       0   0
Gi1/0/28       0   0
Gi1/0/29       0   0
Gi1/0/30       0   0
Gi1/0/31       0   0
Gi1/0/32       0   0
Gi1/0/33       0   0
Gi1/0/34       0   0
Gi1/0/35       0   0
Gi1/0/36       0   0
Te1/0/37       0   0
Te1/0/38       0   0
Te1/0/39       0   0
Te1/0/40       0   0
Te1/0/41       0   0
Te1/0/42       0   0
Te1/0/43       0   0
Te1/0/44       0   0
```

```
Te1/0/45        0   0
Te1/0/46        0   0
Te1/0/47        0   0
Te1/0/48        0   0
Te1/1/1        0   0
Te1/1/2        0   0
Te1/1/3        0   0
Te1/1/4        0   0

Total Ports : 52
Total Ports Receive Bandwidth Percentage Utilization  : 0
Total Ports Transmit Bandwidth Percentage Utilization : 0

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

switch *node*	(optional) Only a single switch may be specified. Default is all switches in a stacked system.
running	(optional) Specifies information on the files currently running.
provisioned	(optional)Specifies information on the software files that are provisioned.
installed	Specifies information on the software installed on the RP
user-interface	Specifies information on the files related to the user-interface.

Command Default

No default behavior or values.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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-type>
processor (revision <processor-revision-id>) with <free-DRAM-memory>
K/<packet-memory>K bytes of memory.
Processor board ID <ID-number

<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.
```

```
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:

------------------------------------------------------------------------------
Technology-package                                      Technology-package
Current                       Type                         Next reboot
------------------------------------------------------------------------------
network-advantage       Smart License                    network-advantage
dna-advantage           Subscription Smart License       dna-advantage


Smart Licensing Status: UNREGISTERED/EVAL MODE

cisco C9300-24U (X86) processor with 1415813K/6147K bytes of memory.
Processor board ID FCW2125L0BH
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:.
```

```
Base Ethernet MAC Address          : 70:d3:79:be:6c:80
Motherboard Assembly Number        : 73-17954-06
Motherboard Serial Number          : FOC21230KPX
Model Revision Number              : A0
Motherboard Revision Number        : A0
Model Number                       : C9300-24U
System Serial Number               : FCW2125L0BH


Switch Ports Model              SW Version        SW Image              Mode
------ ----- -----              ----------        ----------            ----
*    1 40    C9300-24U          16.10.1           CAT9K_IOSXE           INSTALL
     2 40    C9300-24U          16.10.1           CAT9K_IOSXE           INSTALL


Switch 02
---------
Switch uptime                      : 20 hours, 8 minutes

Base Ethernet MAC Address          : 70:d3:79:84:85:80
Motherboard Assembly Number        : 73-17954-06
Motherboard Serial Number          : FOC21230KPK
Model Revision Number              : A0
Motherboard Revision Number        : A0
Model Number                       : C9300-24U
System Serial Number               : FCW2125L03W
Last reload reason                 : Image Install

Configuration register is 0x102
```

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: mcpre
  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: mcpre
  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
```

```
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: 10827f9f9db3b016d19a926acc6be0541440b8d7

Package: rpbase, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status:
 active
  Role: rp_daemons
  File: /flash/cat9k-rpbase.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
 on: RP0/0
  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:
 active
  Role: rp_iosd
  File: /flash/cat9k-rpbase.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
 on: RP0/0
  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:
 active
  Role: rp_security
  File: /flash/cat9k-rpbase.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
 on: RP0/0
  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:
 active
  Role: rp_webui
  File: /flash/cat9k-webui.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
 on: RP0/0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: 5112d7749b38fa1e122ce6ee1bfb266ad7eb553a

Package: srdriver, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status:
 active
  Role: srdriver
  File:
/flash/cat9k-srdriver.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg, on:
 RP0/0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: aff411e981a8dfc8de14005cc33462dc69f8bfaf

Package: cc_srdriver, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2,
status: active
  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
```

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
```

```
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: 10827f9f9db3b016d19a926acc6be0541440b8d7

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_iosd
  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: 5112d7749b38fa1e122ce6ee1bfb266ad7eb553a

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
```

```
  File SHA1 checksum: ada21bb3d57e1b03e5af2329503ed6caa7236d6e

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: aff411e981a8dfc8de14005cc33462dc69f8bfaf

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: 1a2317485f285a3945b31ae57aa64c56ed30a8c0

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: ce821195f0c0bd5e44f21e32fca76cf9b2eed02b

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 155: Table 5, show version running Field Descriptions

Field	Description
Package:	The individual sub-package name.
version:	The individual sub-package version.
status:	Reveals if the package is active or inactive for the specific Supervisor module.
File:	The filename of the individual package file.
on:	The slot number of the Active or Standby Supervisor that this package is running on.
Built:	The date the individual package was built.

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 156: Default Values for the Temperature Thresholds

Device	Difference between Yellow and Red	Red[10]
	14°C	60°C

[10] You cannot configure the red temperature threshold.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

You cannot configure the green and red thresholds but can configure the yellow threshold. Use the **system env temperature threshold yellow** *value* global configuration command to specify the difference between the yellow and red thresholds and to configure the yellow threshold. For example, if the red threshold is 66 degrees C and you want to configure the yellow threshold as 51 degrees C, set the difference between the thresholds as 15 by using the **system env temperature threshold yellow 15** command. For example, if the red threshold is 60 degrees C and you want to configure the yellow threshold as 51 degrees C, set the difference between the thresholds as 15 by using the **system env temperature threshold yellow 9** command.

Note The internal temperature sensor in the device measures the internal system temperature and might vary ±5 degrees C.

Examples

This example sets 15 as the difference between the yellow and red thresholds:

```
Device(config)# system env temperature threshold yellow 15
Device(config)#
```

traceroute mac

To display the Layer 2 path taken by the packets from the specified source MAC address to the specified destination MAC address, use the **traceroute mac** command in privileged EXEC mode.

traceroute mac [**interface** *interface-id*] *source-mac-address* [**interface** *interface-id*] *destination-mac-address* [**vlan** *vlan-id*] [**detail**]

Syntax Description

interface *interface-id*	(Optional) Specifies an interface on the source or destination device.
source-mac-address	The MAC address of the source device in hexadecimal format.
destination-mac-address	The MAC address of the destination device in hexadecimal format.
vlan *vlan-id*	(Optional) Specifies the VLAN on which to trace the Layer 2 path that the packets take from the source device to the destination device. Valid VLAN IDs are 1 to 4094.
detail	(Optional) Specifies that detailed information appears.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

For Layer 2 traceroute to function properly, Cisco Discovery Protocol (CDP) must be enabled on all of the devices in the network. Do not disable CDP.

When the device detects a device in the Layer 2 path that does not support Layer 2 traceroute, the device continues to send Layer 2 trace queries and lets them time out.

The maximum number of hops identified in the path is ten.

Layer 2 traceroute supports only unicast traffic. If you specify a multicast source or destination MAC address, the physical path is not identified, and an error message appears.

The **traceroute mac** command output shows the Layer 2 path when the specified source and destination addresses belong to the same VLAN.

If you specify source and destination addresses that belong to different VLANs, the Layer 2 path is not identified, and an error message appears.

If the source or destination MAC address belongs to multiple VLANs, you must specify the VLAN to which both the source and destination MAC addresses belong.

If the VLAN is not specified, the path is not identified, and an error message appears.

The Layer 2 traceroute feature is not supported when multiple devices are attached to one port through hubs (for example, multiple CDP neighbors are detected on a port).

When more than one CDP neighbor is detected on a port, the Layer 2 path is not identified, and an error message appears.

This feature is not supported in Token Ring VLANs.

Examples

This example shows how to display the Layer 2 path by specifying the source and destination MAC addresses:

```
Device# traceroute mac 0000.0201.0601 0000.0201.0201
  Source 0000.0201.0601 found on con6[WS-C3750E-24PD] (2.2.6.6)
  con6 (2.2.6.6) :Gi0/0/1 => Gi0/0/3
  con5                (2.2.5.5        )  :    Gi0/0/3 => Gi0/0/1
  con1                (2.2.1.1        )  :    Gi0/0/1 => Gi0/0/2
  con2                (2.2.2.2        )  :    Gi0/0/2 => Gi0/0/1
  Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
  Layer 2 trace completed
```

This example shows how to display the Layer 2 path by using the **detail** keyword:

```
Device# traceroute mac 0000.0201.0601 0000.0201.0201 detail
  Source 0000.0201.0601 found on con6[WS-C3750E-24PD] (2.2.6.6)
  con6 / WS-C3750E-24PD / 2.2.6.6 :
          Gi0/0/2 [auto, auto] => Gi0/0/3 [auto, auto]
  con5 / WS-C2950G-24-EI / 2.2.5.5 :
          Fa0/3 [auto, auto] => Gi0/1 [auto, auto]
  con1 / WS-C3550-12G / 2.2.1.1 :
          Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
  con2 / WS-C3550-24 / 2.2.2.2 :
          Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
  Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
  Layer 2 trace completed.
```

This example shows how to display the Layer 2 path by specifying the interfaces on the source and destination devices:

```
Device# traceroute mac interface fastethernet0/1 0000.0201.0601 interface fastethernet0/3
0000.0201.0201
  Source 0000.0201.0601 found on con6[WS-C3750E-24PD] (2.2.6.6)
  con6 (2.2.6.6) :Gi0/0/1 => Gi0/0/3
  con5                (2.2.5.5        )  :    Gi0/0/3 => Gi0/0/1
  con1                (2.2.1.1        )  :    Gi0/0/1 => Gi0/0/2
  con2                (2.2.2.2        )  :    Gi0/0/2 => Gi0/0/1
  Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
  Layer 2 trace completed
```

This example shows the Layer 2 path when the device is not connected to the source device:

```
Device# traceroute mac 0000.0201.0501 0000.0201.0201 detail
  Source not directly connected, tracing source .....
  Source 0000.0201.0501 found on con5[WS-C3750E-24TD] (2.2.5.5)
  con5 / WS-C3750E-24TD / 2.2.5.5 :
          Gi0/0/1 [auto, auto] => Gi0/0/3 [auto, auto]
```

```
  con1 / WS-C3550-12G / 2.2.1.1 :
         Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
  con2 / WS-C3550-24 / 2.2.2.2 :
         Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
  Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
  Layer 2 trace completed.
```

This example shows the Layer 2 path when the device cannot find the destination port for the source MAC address:

```
Device# traceroute mac 0000.0011.1111 0000.0201.0201
  Error:Source Mac address not found.
  Layer2 trace aborted.
```

This example shows the Layer 2 path when the source and destination devices are in different VLANs:

```
Device# traceroute mac 0000.0201.0601 0000.0301.0201
  Error:Source and destination macs are on different vlans.
  Layer2 trace aborted.
```

This example shows the Layer 2 path when the destination MAC address is a multicast address:

```
Device# traceroute mac 0000.0201.0601 0100.0201.0201
  Invalid destination mac address
```

This example shows the Layer 2 path when source and destination devices belong to multiple VLANs:

```
Device# traceroute mac 0000.0201.0601 0000.0201.0201
  Error:Mac found on multiple vlans.
  Layer2 trace aborted.
```

traceroute mac ip

To display the Layer 2 path taken by the packets from the specified source IP address or hostname to the specified destination IP address or hostname, use the **traceroute mac ip** command in privileged EXEC mode.

traceroute mac ip {*source-ip-address source-hostname*} {*destination-ip-address destination-hostname*} [**detail**]

Syntax Description

source-ip-address	The IP address of the source device as a 32-bit quantity in dotted-decimal format.
source-hostname	The IP hostname of the source device.
destination-ip-address	The IP address of the destination device as a 32-bit quantity in dotted-decimal format.
destination-hostname	The IP hostname of the destination device.
detail	(Optional) Specifies that detailed information appears.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

For Layer 2 traceroute to function properly, Cisco Discovery Protocol (CDP) must be enabled on each device in the network. Do not disable CDP.

When the device detects a device in the Layer 2 path that does not support Layer 2 traceroute, the device continues to send Layer 2 trace queries and lets them time out.

The maximum number of hops identified in the path is ten.

The **traceroute mac ip** command output shows the Layer 2 path when the specified source and destination IP addresses are in the same subnet.

When you specify the IP addresses, the device uses Address Resolution Protocol (ARP) to associate the IP addresses with the corresponding MAC addresses and the VLAN IDs.

- If an ARP entry exists for the specified IP address, the device uses the associated MAC address and identifies the physical path.
- If an ARP entry does not exist, the device sends an ARP query and tries to resolve the IP address. The IP addresses must be in the same subnet. If the IP address is not resolved, the path is not identified, and an error message appears.

The Layer 2 traceroute feature is not supported when multiple devices are attached to one port through hubs (for example, multiple CDP neighbors are detected on a port).

When more than one CDP neighbor is detected on a port, the Layer 2 path is not identified, and an error message appears.

This feature is not supported in Token Ring VLANs.

Examples

This example shows how to display the Layer 2 path by specifying the source and destination IP addresses and by using the **detail** keyword:

```
Device# traceroute mac ip 2.2.66.66 2.2.22.22 detail
Translating IP to mac .....
2.2.66.66 => 0000.0201.0601
2.2.22.22 => 0000.0201.0201

Source 0000.0201.0601 found on con6[WS-C2950G-24-EI] (2.2.6.6)
con6 / WS-C3750E-24TD / 2.2.6.6 :
        Gi0/0/1 [auto, auto] => Gi0/0/3 [auto, auto]
con5 / WS-C2950G-24-EI / 2.2.5.5 :
        Fa0/3 [auto, auto] => Gi0/1 [auto, auto]
con1 / WS-C3550-12G / 2.2.1.1 :
        Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2 / WS-C3550-24 / 2.2.2.2 :
        Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
```

This example shows how to display the Layer 2 path by specifying the source and destination hostnames:

```
Device# traceroute mac ip con6 con2
Translating IP to mac .....
2.2.66.66 => 0000.0201.0601
2.2.22.22 => 0000.0201.0201

Source 0000.0201.0601 found on con6
con6 (2.2.6.6) :Gi0/0/1 => Gi0/0/3
con5                 (2.2.5.5        )  :    Gi0/0/3 => Gi0/1
con1                 (2.2.1.1        )  :    Gi0/0/1 => Gi0/2
con2                 (2.2.2.2        )  :    Gi0/0/2 => Fa0/1
Destination 0000.0201.0201 found on con2
Layer 2 trace completed
```

This example shows the Layer 2 path when ARP cannot associate the source IP address with the corresponding MAC address:

```
Device# traceroute mac ip 2.2.66.66 2.2.77.77
Arp failed for destination 2.2.77.77.
Layer2 trace aborted.
```

type

To display the contents of one or more files, use the **type** command in boot loader mode.

type *filesystem:/file-url...*

Syntax Description

filesystem:	Alias for a file system. Use **flash:** for the system board flash device; use **usbflash0:** for USB memory sticks.
/file-url...	Path (directory) and name of the files to display. Separate each filename with a space.

Command Default

No default behavior or values.

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Filenames and directory names are case sensitive.

If you specify a list of files, the contents of each file appear sequentially.

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:
```

unset

To reset one or more environment variables, use the **unset** command in boot loader mode.

unset *variable...*

Syntax Description

variable	Use one of these keywords for *variable*: **MANUAL_BOOT**—Specifies whether the device automatically or manually boots.
	BOOT—Resets the list of executable files to try to load and execute when automatically booting. If the BOOT environment variable is not set, the system attempts to load and execute the first executable image it can find by using a recursive, depth-first search through the flash: file system. If the BOOT variable is set but the specified images cannot be loaded, the system attempts to boot the first bootable file that it can find in the flash: file system.
	ENABLE_BREAK—Specifies whether the automatic boot process can be interrupted by using the **Break** key on the console after the flash: file system has been initialized.
	HELPER—Identifies the semicolon-separated list of loadable files to dynamically load during the boot loader initialization. Helper files extend or patch the functionality of the boot loader.
	PS1—Specifies the string that is used as the command-line prompt in boot loader mode.
	CONFIG_FILE—Resets the filename that Cisco IOS uses to read and write a nonvolatile copy of the system configuration.
	BAUD—Resets the rate in bits per second (b/s) used for the console. The Cisco IOS software inherits the baud rate setting from the boot loader and continues to use this value unless the configuration file specifies another setting.

Command Default

No default behavior or values.

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Under typical circumstances, it is not necessary to alter the setting of the environment variables.

The MANUAL_BOOT environment variable can also be reset by using the **no boot manual** global configuration command.

The BOOT environment variable can also be reset by using the **no boot system** global configuration command.

The ENABLE_BREAK environment variable can also be reset by using the **no boot enable-break** global configuration command.

The HELPER environment variable can also be reset by using the **no boot helper** global configuration command.

The CONFIG_FILE environment variable can also be reset by using the **no boot config-file** global configuration command.

Example

This example shows how to unset the SWITCH_PRIORITY environment variable:

```
Device: unset SWITCH_PRIORITY
```

version

To display the boot loader version, use the **version** command in boot loader mode.

version [*-v*]

Syntax Description

-v	Displays Hardware Anchor, Microloader, Firmware-DDR and ROMMON Revision versions.

Command Default

No default behavior or values.

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Examples

This example shows how to display the boot loader version on a device:

```
Device: version -v
System Bootstrap, Version 16.10.1r, RELEASE SOFTWARE (P)
Compiled Tue 09/04/2018 22:58:10 by rel

Current ROMMON image : Primary
C9200-48P-4X platform with 2097152 Kbytes of main memory

HARDWARE ANCHOR : v027.0  crayprod_20160517 20160517-2135
MICROLOADER     : v061.0  rel_16_10_1r 20180904-2252
FIRMWARE-DDR    : v011.0  rel_16_10_1r 20180904-2254
ROMMON REVISION : v010.003
```

Tracing

- Information About Tracing, on page 1638
- set platform software trace, on page 1640
- show platform software trace filter-binary, on page 1644
- show platform software trace message, on page 1645
- show platform software trace level, on page 1648
- request platform software trace archive, on page 1651
- request platform software trace rotate all, on page 1652
- request platform software trace filter-binary, on page 1653

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 157: Tracing Levels and Descriptions

Tracing Level	Description
Emergency	The message is regarding an issue that makes the system unusable.
Error	The message is regarding a system error.
Warning	The message is regarding a system warning.
Notice	The message is regarding a significant issue, but the switch is still working normally.
Informational	The message is useful for informational purposes only.
Debug	The message provides debug-level output.
Verbose	All possible trace messages are sent.
Noise	All possible trace messages for the module are logged. The noise level is always equal to the highest possible tracing level. Even if a future enhancement to tracing introduces a higher tracing level, the noise level will become equal to the level of that new enhancement.

set platform software trace

To set the trace level for a specific module within a process, use the **set platform software trace** command in privileged EXEC or user EXEC mode.

set platform software trace *process slot module trace-level*

Syntax Description

process	Process whose tracing level is being set. Options include: • **chassis-manager**—The Chassis Manager process. • **cli-agent**—The CLI Agent process. • **dbm**—The Database Manager process. • **emd**—The Environmental Monitoring process. • **fed**—The Forwarding Engine Driver process. • **forwarding-manager**—The Forwarding Manager process. • **host-manager**—The Host Manager process. • **iomd**—The Input/Output Module daemon (IOMd) process. • **ios**—The IOS process. • **license-manager**—The License Manager process. • **logger**—The Logging Manager process. • **platform-mgr**—The Platform Manager process. • **pluggable-services**—The Pluggable Services process. • **replication-mgr**—The Replication Manager process. • **shell-manager**—The Shell Manager process. • **smd**—The Session Manager process. • **table-manager**—The Table Manager Server. • **wireshark**—The Embedded Packet Capture (EPC) Wireshark process.

slot	Hardware slot where the process for which the trace level is set, is running. Options include: • *number*—Number of the SIP slot of the hardware module where the trace level is set. For instance, if you want to specify the SIP in SIP slot 2 of the switch, enter 2. • *SIP-slot / SPA-bay*—Number of the SIP switch slot and the number of the shared port adapter (SPA) bay of that SIP. For instance, if you want to specify the SPA in bay 2 of the SIP in switch slot 3, enter 3/2. • **F0**—The Embedded-Service-Processor in slot 0. • **FP active**—The active Embedded-Service-Processor. • **R0**—The route processor in slot 0. • **RP active**—The active route processor. • **switch** <*number*> —The switch with its number specified. • **switch active**—The active switch. • **switch standby**—The standby switch.
module	Module within the process for which the tracing level is set.

trace-level	Trace level. Options include: • **debug**—Debug level tracing. A debug-level trace message is a non-urgent message providing a large amount of detail about the module. • **emergency**—Emergency level tracing. An emergency-level trace message is a message indicating that the system is unusable. • **error**—Error level tracing. An error-level tracing message is a message indicating a system error. • **info**—Information level tracing. An information-level tracing message is a non-urgent message providing information about the system. • **noise**—Noise level tracing. The noise level is always equal to the highest tracing level possible and always generates every possible tracing message. The noise level is always equal to the highest-level tracing message possible for a module, even if future enhancements to this command introduce options that allow users to set higher tracing levels. • **notice**—The message is regarding a significant issue, but the switch is still working normally. • **verbose**—Verbose level tracing. All possible tracing messages are sent when the trace level is set to verbose. • **warning**—Warning messages.

Command Default

The default tracing level for all modules is **notice**.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
	This command was introduced.

Usage Guidelines

The *module* options vary by process and by *hardware-module*. Use the ? option when entering this command to see which *module* options are available with each keyword sequence.

Use the **show platform software trace message** command to view trace messages.

Trace files are stored in the tracelogs directory in the harddisk: file system. These files can be deleted without doing any harm to your switch operation.

Trace file output is used for debugging. The trace level is a setting that determines how much information should be stored in trace files about a module.

Examples

This example shows how to set the trace level for all the modules in dbm process:

```
# set platform software trace dbm R0 all-modules debug
```

show platform software trace filter-binary

To display the most recent trace information for a specific module, use the **show platform software trace filter-binary** command in privileged EXEC or user EXEC mode.

show platform software trace filter-binary*modules* [**context** *mac-address*]

Syntax Description

context*mac-address*	Represents the context used to filter. Additionally, you can filter based on module names and trace levels. The context keyword accepts either a MAC address or any other argument based on which a trace is tagged.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
	This command was introduced.

Usage Guidelines

This command collates and sorts all the logs present in the `/tmp/.../` across all the processes relevant to the module. The trace logs of all the processes relevant to the specified module are printed to the console. This command also generates a file named `collated_log_{system time}` with the same content, in the `/crashinfo/tracelogs` directory.

show platform software trace message

To display the trace messages for a process, use the **set platform software trace** command in privileged EXEC or user EXEC mode.

show platform software trace message *process slot*

Syntax Description

process	Tracing level that is being set. Options include: • **chassis-manager**—The Chassis Manager process. • **cli-agent**—The CLI Agent process. • **cmm**—The CMM process. • **dbm**—The Database Manager process. • **emd**—The Environmental Monitoring process. • **fed**—The Forwarding Engine Driver process. • **forwarding-manager**—The Forwarding Manager process. • **geo**—The Geo Manager process. • **host-manager**—The Host Manager process. • **interface-manager**—The Interface Manager process. • **iomd**—The Input/Output Module daemon (IOMd) process. • **ios**—The IOS process. • **license-manager**—The License Manager process. • **logger**—The Logging Manager process. • **platform-mgr**—The Platform Manager process. • **pluggable-services**—The Pluggable Services process. • **replication-mgr**—The Replication Manager process. • **shell-manager**—The Shell Manager process. • **sif**—The Stack Interface (SIF) Manager process. • **smd**—The Session Manager process. • **stack-mgr**—The Stack Manager process. • **table-manager**—The Table Manager Server. • **thread-test**—The Multithread Manager process. • **virt-manager**—The Virtualization Manager process.

slot	Hardware slot where the process for which the trace level is set, is running. Options include:
	• *number*—Number of the SIP slot of the hardware module where the trace level is set. For instance, if you want to specify the SIP in SIP slot 2 of the switch, enter 2.
	• *SIP-slot / SPA-bay*—Number of the SIP switch slot and the number of the shared port adapter (SPA) bay of that SIP. For instance, if you want to specify the SPA in bay 2 of the SIP in switch slot 3, enter 3/2.
	• **F0**—The Embedded Service Processor slot 0.
	• **FP active**—The active Embedded Service Processor.
	• **R0**—The route processor in slot 0.
	• **RP active**—The active route processor.
	• **switch** <*number*> —The switch, with its number specified.
	• **switch active**—The active switch.
	• **switch standby**—The standby switch.
	  • *number*—Number of the SIP slot of the hardware module where the trace level is set. For instance, if you want to specify the SIP in SIP slot 2 of the switch, enter 2.
	  • *SIP-slot / SPA-bay*—Number of the SIP switch slot and the number of the shared port adapter (SPA) bay of that SIP. For instance, if you want to specify the SPA in bay 2 of the SIP in switch slot 3, enter 3/2.
	  • **F0**—The Embedded Service Processor in slot 0.
	  • **FP active**—The active Embedded Service Processor.
	  • **R0**—The route processor in slot 0.
	  • **RP active**—The active route processor.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
	This command was introduced.

Examples

This example shows how to display the trace messages for the Stack Manager and the Forwarding Engine Driver processes:

```
# show platform software trace message stack-mgr switch active R0
10/30 09:42:48.767 [btrace] [8974]: (note): Successfully registered module [97] [uiutil]
10/30 09:42:48.762 [btrace] [8974]: (note): Successfully registered module [98]
[tdl_cdlcore_message]
10/29 13:28:19.023 [stack_mgr] [8974]: (note): Examining peer state
10/29 13:28:19.023 [stack_mgr] [8974]: (note): no switch eligible for standby election
presently
10/29 13:28:19.022 [stack_mgr] [8974]: (note): Posting event
stack_fsm_event_wait_standby_elect_timer_expired, curstate stack_fsm_state_active_ready
10/29 13:28:19.022 [stack_mgr] [8974]: (note): Timer HDL - STACK_WAIT_STANDBY_ELECT_TIMER
expired
10/29 13:26:46.584 [btrace] [8974]: (note): Successfully registered module [99]
[tdl_ui_message]
10/29 13:26:46.582 [bipc] [8974]: (note): Pending connection to server 10.129.1.0
10/29 13:26:36.582 [evutil] [8974]: (ERR): Connection attempt for sman-ui-serv (uipeer
uplink to slot 1) failed, invoking disconnect
10/29 13:26:36.582 [evutil] [8974]: (ERR): Asynchronous connect failed for [uipeer uplink
to slot 1] (fd == -1)
10/29 13:26:36.581 [bipc] [8974]: (note): Pending connection to server 10.129.1.0
10/29 13:26:26.581 [evutil] [8974]: (ERR): Connection attempt for sman-ui-serv (uipeer
uplink to slot 1) failed, invoking disconnect

# show platform software trace message fed switch active
11/02 10:55:01.832 [btrace]: [11310]:  UUID: 0, ra: 0 (note): Successfully registered module
 [86] [uiutil]
11/02 10:55:01.848 [btrace]: [11310]:  UUID: 0, ra: 0 (note): Single message size is greater
 than 1024
11/02 10:55:01.822 [btrace]: [11310]:  UUID: 0, ra: 0 (note): Successfully registered module
 [87] [tdl_cdlcore_message]
11/01 09:54:41.474 [btrace]: [12312]:  UUID: 0, ra: 0 (note): Successfully registered module
 [88] [tdl_ngwc_gold_message]
11/01 09:54:11.228 [btrace]: [12312]:  UUID: 0, ra: 0 (note): Successfully registered module
 [89] [tdl_doppler_iosd_matm_type]
11/01 09:53:37.454 [btrace]: [11310]:  UUID: 0, ra: 0 (note): Successfully registered module
 [90] [tdl_ui_message]
11/01 09:53:37.382 [bipc]: [11310]:  UUID: 0, ra: 0 (note): Pending connection to server
10.129.1.0
11/01 09:53:34.227 [xcvr]: [18846]:  UUID: 0, ra: 0 (ERR): FRU hardware authentication Fail,
 result = 1.
11/01 09:53:33.775 [ng3k_scc]: [18846]:  UUID: 0, ra: 0 (ERR): SMART COOKIE: SCC I2C receive
 failed: rc=10
11/01 09:53:33.775 [ng3k_scc]: [18846]:  UUID: 0, ra: 0 (ERR):
SMART COOKIE receive failed, try again
11/01 09:53:33.585 [ng3k_scc]: [18846]:  UUID: 0, ra: 0 (ERR):
```

show platform software trace level

To view the trace levels for all the modules under a specific process, use the **show platform software trace level** command in privileged EXEC or user EXEC mode.

show platform software trace level *process slot*

Syntax Description

process	Process whose tracing level is being set. Options include: • **chassis-manager**—The Chassis Manager process. • **cli-agent**—The CLI Agent process. • **cmm**—The CMM process. • **dbm**—The Database Manager process. • **emd**—The Environmental Monitoring process. • **fed**—The Forwarding Engine Driver process. • **forwarding-manager**—The Forwarding Manager process. • **geo**—The Geo Manager process. • **host-manager**—The Host Manager process. • **interface-manager**—The Interface Manager process. • **iomd**—The Input/Output Module daemon (IOMd) process. • **ios**—The IOS process. • **license-manager**—The License Manager process. • **logger**—The Logging Manager process. • **platform-mgr**—The Platform Manager process. • **pluggable-services**—The Pluggable Services process. • **replication-mgr**—The Replication Manager process. • **shell-manager**—The Shell Manager process. • **sif**—The Stack Interface (SIF) Manager process. • **smd**—The Session Manager process. • **stack-mgr**—The Stack Manager process. • **table-manager**—The Table Manager Server. • **thread-test**—The Multithread Manager process. • **virt-manager**—The Virtualization Manager process.

slot	Hardware slot where the process for which the trace level is set, is running. Options include:
	• *number*—Number of the SIP slot of the hardware module where the trace level is set. For instance, if you want to specify the SIP in SIP slot 2 of the switch, enter 2.
	• *SIP-slot / SPA-bay*—Number of the SIP switch slot and the number of the shared port adapter (SPA) bay of that SIP. For instance, if you want to specify the SPA in bay 2 of the SIP in switch slot 3, enter 3/2.
	• **F0**—The Embedded Service Processor in slot 0.
	• **F1**—The Embedded Service Processor in slot 1.
	• **FP active**—The active Embedded Service Processor.
	• **R0**—The route processor in slot 0.
	• **RP active**—The active route processor.
	• **switch** <*number*> —The switch, with its number specified.
	• **switch active**—The active switch.
	• **switch standby**—The standby switch.
	  • *number*—Number of the SIP slot of the hardware module where the trace level is set. For instance, if you want to specify the SIP in SIP slot 2 of the switch, enter 2.
	  • *SIP-slot / SPA-bay*—Number of the SIP switch slot and the number of the shared port adapter (SPA) bay of that SIP. For instance, if you want to specify the SPA in bay 2 of the SIP in switch slot 3, enter 3/2.
	  • **F0**—The Embedded Service Processor in slot 0.
	  • **FP active**—The active Embedded Service Processor.
	  • **R0**—The route processor in slot 0.
	  • **RP active**—The active route processor.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
	This command was introduced.

Examples

This example shows how to view the trace level:

```
# show platform software trace level dbm switch active R0
```

```
Module Name                      Trace Level
-------------------------------------------------
binos                            Notice
binos/brand                      Notice
bipc                             Notice
btrace                           Notice
bump_ptr_alloc                   Notice
cdllib                           Notice
chasfs                           Notice
dbal                             Informational
dbm                              Debug
evlib                            Notice
evutil                           Notice
file_alloc                       Notice
green-be                         Notice
ios-avl                          Notice
klib                             Debug
services                         Notice
sw_wdog                          Notice
syshw                            Notice
tdl_cdlcore_message              Notice
tdl_dbal_root_message            Notice
tdl_dbal_root_type               Notice
```

request platform software trace archive

To archive all the trace logs relevant to all the processes running on a system since the last reload on the switch and to save this in the specified location, use the **request platform software trace archive** command in privileged EXEC or user EXEC mode.

request platform software trace archive [**last** *number-of-days* [**days** [**target** *location*]] | **target** *location*]

Syntax Description

last *number-of-days*	Specifies the number of days for which the trace files have to be archived.
target *location*	Specifies the location and name of the archive file.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
	This command was introduced.

Usage Guidelines

This archive file can be copied from the system, using the tftp or scp commands.

Examples

This example shows how to archive all the trace logs of the processes running on the switch since the last 5 days:

```
# request platform software trace archive last 5 days target flash:test_archive
```

request platform software trace rotate all

To rotate all the current in-memory trace logs into the crashinfo partition and start a new in-memory trace log for each process, use the **request platform software trace rotate all** command in privileged EXEC or user EXEC mode.

request platform software trace rotate all

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
	This command was introduced.

Usage Guidelines

The trace log files are for read-only purpose. Do not edit the contents of the file. If there is a requirement to delete the contents of the file to view certain set of logs, use this command to start a new trace log file.

Examples

This example shows how to rotate all the in-memory trace logs of the processes running on the switch since the last one day:

```
# request platform software trace slot switch active R0 archive last 1 days target flash:test
```

request platform software trace filter-binary

To collate and sort all the archived logs present in the tracelogs subdirectory, use the **request platform software trace filter-binary** command in privileged EXEC or user EXEC mode.

request platform software trace filter-binary *modules* [**context** *mac-address*]

Syntax Description

context *mac-address*	Represents the context used to filter. Additionally, you can filter based on module names and trace levels. The context keyword accepts either a MAC address or any other argument based on which a trace is tagged.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
	This command was introduced.

Usage Guidelines

This command collates and sorts all the archived logs present in the tracelogs subdirectory, across all the processes relevant to the module. This command also generates a file named `collated_log_{system time}` with the same content, in the `/crashinfo/tracelogs` directory.

PART XIII

VLAN

- VLAN Commands, on page 1657

VLAN Commands

- clear vtp counters, on page 1658
- debug sw-vlan, on page 1659
- debug sw-vlan ifs, on page 1661
- debug sw-vlan notification, on page 1662
- debug sw-vlan vtp, on page 1663
- private-vlan, on page 1665
- private-vlan mapping, on page 1667
- show interfaces private-vlan mapping, on page 1669
- show vlan, on page 1670
- show vtp, on page 1674
- switchport mode private-vlan, on page 1679
- switchport priority extend, on page 1681
- switchport trunk, on page 1682
- vlan, on page 1685
- vlan dot1q tag native, on page 1691
- vtp (global configuration), on page 1692
- vtp (interface configuration), on page 1697
- vtp primary, on page 1698

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Examples

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

badpmcookies	Displays debug messages for VLAN manager incidents of bad port manager cookies.
cfg-vlan	Displays VLAN configuration debug messages.
bootup	Displays messages when the switch is booting up.
cli	Displays messages when the command-line interface (CLI) is in VLAN configuration mode.
events	Displays debug messages for VLAN manager events.
ifs	Displays debug messages for the VLAN manager IOS file system (IFS). See debug sw-vlan ifs, on page 1661 for more information.
mapping	Displays debug messages for VLAN mapping.
notification	Displays debug messages for VLAN manager notifications. See debug sw-vlan notification, on page 1662 for more information.
packets	Displays debug messages for packet handling and encapsulation processes.
redundancy	Displays debug messages for VTP VLAN redundancy.
registries	Displays debug messages for VLAN manager registries.
vtp	Displays debug messages for the VLAN Trunking Protocol (VTP) code. See debug sw-vlan vtp, on page 1663 for more information.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The **undebug sw-vlan** command is the same as the **no debug sw-vlan** command.

Examples

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The **undebug sw-vlan ifs** command is the same as the **no debug sw-vlan ifs** command.

When selecting the file read operation, Operation **1** reads the file header, which contains the header verification word and the file version number. Operation **2** reads the main body of the file, which contains most of the domain and VLAN information. Operation **3** reads type length version (TLV) descriptor structures. Operation **4** reads TLV data.

Examples

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.

debug sw-vlan notification {**accfwdchange** | **allowedvlancfgchange** | **fwdchange** | **linkchange** | **modechange** | **pruningcfgchange** | **statechange**}
no debug sw-vlan notification {**accfwdchange** | **allowedvlancfgchange** | **fwdchange** | **linkchange** | **modechange** | **pruningcfgchange** | **statechange**}

Syntax Description

accfwdchange	Displays debug messages for VLAN manager notification of aggregated access interface spanning-tree forward changes.
allowedvlancfgchange	Displays debug messages for VLAN manager notification of changes to the allowed VLAN configuration.
fwdchange	Displays debug messages for VLAN manager notification of spanning-tree forwarding changes.
linkchange	Displays debug messages for VLAN manager notification of interface link-state changes.
modechange	Displays debug messages for VLAN manager notification of interface mode changes.
pruningcfgchange	Displays debug messages for VLAN manager notification of changes to the pruning configuration.
statechange	Displays debug messages for VLAN manager notification of interface state changes.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The **undebug sw-vlan notification** command is the same as the **no debug sw-vlan notification** command.

When you enable debugging on a switch stack, it is enabled only on the active switch. To debug a specific stack member, you can start a CLI session from the active switch by using the **session switch** *stack-member-number* privileged EXEC command.

Examples

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.

debug sw-vlan vtp {**events** | **packets** | **pruning** [{**packets** | **xmit**}] | **redundancy** | **xmit**}
no debug sw-vlan vtp {**events** | **packets** | **pruning** | **redundancy** | **xmit**}

Syntax Description

events	Displays debug messages for general-purpose logic flow and detailed VTP messages generated by the VTP_LOG_RUNTIME macro in the VTP code.
packets	Displays debug messages for the contents of all incoming VTP packets that have been passed into the VTP code from the Cisco IOS VTP platform-dependent layer, except for pruning packets.
pruning	Displays debug messages generated by the pruning segment of the VTP code.
packets	(Optional) Displays debug messages for the contents of all incoming VTP pruning packets that have been passed into the VTP code from the Cisco IOS VTP platform-dependent layer.
xmit	(Optional) Displays debug messages for the contents of all outgoing VTP packets that the VTP code requests the Cisco IOS VTP platform-dependent layer to send.
redundancy	Displays debug messages for VTP redundancy.
xmit	Displays debug messages for the contents of all outgoing VTP packets that the VTP code requests the Cisco IOS VTP platform-dependent layer to send, except for pruning packets.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The **undebug sw-vlan vtp** command is the same as the **no debug sw-vlan vtp** command.

If no additional parameters are entered after the **pruning** keyword, VTP pruning debugging messages appear. They are generated by the VTP_PRUNING_LOG_NOTICE, VTP_PRUNING_LOG_INFO, VTP_PRUNING_LOG_DEBUG, VTP_PRUNING_LOG_ALERT, and VTP_PRUNING_LOG_WARNING macros in the VTP pruning code.

When you enable debugging on a switch stack, it is enabled only on the active switch. To debug a specific stack member, you can start a CLI session from the active switch by using the **session switch** *stack-member-number* privileged EXEC command.

Examples

This example shows how to display debug messages for VTP redundancy:

```
Device> enable
Device# debug sw-vlan vtp redundancy
```

private-vlan

To configure private VLANs and to configure the association between private VLAN primary and secondary VLANs, use the **private-vlan** VLAN configuration command on the switch stack or on a standalone switch. Use the **no** form of this command to return the VLAN to normal VLAN configuration.

private-vlan {**association** [{**add** | **remove**}] *secondary-vlan-list* | **community** | **isolated** | **primary**}
no private-vlan {**association** | **community** | **isolated** | **primary**}

Syntax Description

association	Creates an association between the primary VLAN and a secondary VLAN.
add	Associates a secondary VLAN to a primary VLAN.
remove	Clears the association between a secondary VLAN and a primary VLAN.
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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Before configuring private VLANs, you must disable VTP (VTP mode transparent). After you configure a private VLAN, you should not change the VTP mode to client or server.

VTP does not propagate private VLAN configurations. You must manually configure private VLANs on all switches in the Layer 2 network to merge their Layer 2 databases and to prevent flooding of private VLAN traffic.

You cannot include VLAN 1 or VLANs 1002 to 1005 in the private VLAN configuration. Extended VLANs (VLAN IDs 1006 to 4094) can be configured in private VLANs.

You can associate a secondary (isolated or community) VLAN with only one primary VLAN. A primary VLAN can have one isolated VLAN and multiple community VLANs associated with it.

- A secondary VLAN cannot be configured as a primary VLAN.
- The *secondary-vlan-list* cannot contain spaces. It can contain multiple comma-separated items. Each item can be a single private VLAN ID or a hyphenated range of private VLAN IDs. The list can contain one isolated VLAN and multiple community VLANs.

- If you delete either the primary or secondary VLANs, the ports associated with the VLAN become inactive.

A community VLAN carries traffic among community ports and from community ports to the promiscuous ports on the corresponding primary VLAN.

An isolated VLAN is used by isolated ports to communicate with promiscuous ports. It does not carry traffic to other community ports or isolated ports with the same primary VLAN domain.

A primary VLAN is the VLAN that carries traffic from a gateway to customer end stations on private ports.

Configure Layer 3 VLAN interfaces (SVIs) only for primary VLANs. You cannot configure Layer 3 VLAN interfaces for secondary VLANs. SVIs for secondary VLANs are inactive while the VLAN is configured as a secondary VLAN.

The **private-vlan** commands do not take effect until you exit from VLAN configuration mode.

Do not configure private VLAN ports as EtherChannels. While a port is part of the private VLAN configuration, any EtherChannel configuration for it is inactive.

Do not configure a private VLAN as a Remote Switched Port Analyzer (RSPAN) VLAN.

Do not configure a private VLAN as a voice VLAN.

Do not configure fallback bridging on switches with private VLANs.

Although a private VLAN contains more than one VLAN, only one STP instance runs for the entire private VLAN. When a secondary VLAN is associated with the primary VLAN, the STP parameters of the primary VLAN are propagated to the secondary VLAN.

For more information about private VLAN interaction with other features, see the software configuration guide for this release.

This example shows how to configure VLAN 20 as a primary VLAN, VLAN 501 as an isolated VLAN, and VLANs 502 and 503 as community VLANs, and to associate them in a private VLAN:

```
# configure terminal
(config)# vlan 20
(config-vlan)# private-vlan primary
(config-vlan)# exit
(config)# vlan 501
(config-vlan)# private-vlan isolated
(config-vlan)# exit
(config)# vlan 502
(config-vlan)# private-vlan community
(config-vlan)# exit
(config)# vlan 503
(config-vlan)# private-vlan community
(config-vlan)# exit
(config)# vlan 20
(config-vlan)# private-vlan association 501-503
(config-vlan)# end
```

You can verify your setting by entering the **show vlan private-vlan** or **show interfaces status privileged** EXEC command.

private-vlan mapping

To create a mapping between the primary and the secondary VLANs so that both VLANs share the same primary VLAN switched virtual interface (SVI), use the **private-vlan mapping** interface configuration command on a switch virtual interface (SVI). Use the **no** form of this command to remove private VLAN mappings from the SVI.

private-vlan mapping [{**add** | **remove**}] *secondary-vlan-list*
no private-vlan mapping

Syntax Description

add	(Optional) Maps the secondary VLAN to the primary VLAN SVI.
remove	(Optional) Removes the mapping between the secondary VLAN and the primary VLAN SVI.
secondary-vlan-list	One or more secondary VLANs to be mapped to the primary VLAN SVI.

Command Default

No private VLAN SVI mapping is configured.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The device must be in VTP transparent mode when you configure private VLANs.

The SVI of the primary VLAN is created at Layer 3.

Configure Layer 3 VLAN interfaces (SVIs) only for primary VLANs. You cannot configure Layer 3 VLAN interfaces for secondary VLANs. SVIs for secondary VLANs are inactive while the VLAN is configured as a secondary VLAN.

The *secondary-vlan-list* argument cannot contain spaces. It can contain multiple comma-separated items. Each item can be a single private VLAN ID or a hyphenated range of private VLAN IDs. The list can contain one isolated VLAN and multiple community VLANs.

Traffic that is received on the secondary VLAN is routed by the SVI of the primary VLAN.

A secondary VLAN can be mapped to only one primary SVI. If you configure the primary VLAN as a secondary VLAN, all SVIs specified in this command are brought down.

If you configure a mapping between two VLANs that do not have a valid Layer 2 private VLAN association, the mapping configuration does not take effect.

Examples

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 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	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Examples

This example shows how to display the information about the private VLAN mapping:

```
Device#show interfaces private-vlan mapping
Interface Secondary VLAN Type
--------- -------------- -----------------
vlan2     301            community
vlan3     302            community
```

show 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** | **group** | **id** *vlan-id* | **mtu** | **name** *vlan-name* | **private-vlan** [{**type**}] | **remote-span** | **summary**}]

Syntax Description

brief	(Optional) Displays one line for each VLAN with the VLAN name, status, and its ports.
group	(Optional) Displays information about VLAN groups.
id *vlan-id*	(Optional) Displays information about a single VLAN identified by the VLAN ID number. For *vlan-id*, the range is 1 to 4094.
mtu	(Optional) Displays a list of VLANs and the minimum and maximum transmission unit (MTU) sizes configured on ports in the VLAN.
name *vlan-name*	(Optional) Displays information about a single VLAN identified by the VLAN name. The VLAN name is an ASCII string from 1 to 32 characters.
private-vlan	(Optional) Displays information about configured private VLANs, including primary and secondary VLAN IDs, type (community, isolated, or primary) and ports belonging to the private VLAN. This keyword is only supported if your switch is running the IP services feature set.
type	(Optional) Displays only private VLAN ID and type.
remote-span	(Optional) Displays information about Remote SPAN (RSPAN) VLANs.
summary	(Optional) Displays VLAN summary information.

Note The **ifindex** keyword is not supported, even though it is visible in the command-line help string.

Command Modes

User EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

In the **show vlan mtu** command output, the MTU_Mismatch column shows whether all the ports in the VLAN have the same MTU. When yes appears in the column, it means that the VLAN has ports with different MTUs, and packets that are switched from a port with a larger MTU to a port with a smaller MTU might be dropped.

If the VLAN does not have an SVI, the hyphen (-) symbol appears in the SVI_MTU column. If the MTU-Mismatch column displays yes, the names of the ports with the MinMTU and the MaxMTU appear.

If you try to associate a private VLAN secondary VLAN with a primary VLAN before you define the secondary VLAN, the secondary VLAN is not included in the **show vlan private-vlan** command output.

In the **show vlan private-vlan type** command output, a type displayed as normal means a VLAN that has a private VLAN association but is not part of the private VLAN. For example, if you define and associate two VLANs as primary and secondary VLANs and then delete the secondary VLAN configuration without removing the association from the primary VLAN, the VLAN that was the secondary VLAN is shown as normal in the display. In the **show vlan private-vlan** output, the primary and secondary VLAN pair is shown as nonoperational.

Examples

This is an example of output from the **show vlan** command. See the table that follows for descriptions of the fields in the display.

```
Device> show vlan
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi1/0/2, Gi1/0/3, Gi1/0/4
                                                Gi1/0/5, Gi1/0/6, Gi1/0/7
                                                Gi1/0/8, Gi1/0/9, Gi1/0/10
                                                Gi1/0/11, Gi1/0/12, Gi1/0/13
                                                Gi1/0/14, Gi1/0/15, Gi1/0/16
                                                Gi1/0/17, Gi1/0/18, Gi1/0/19
                                                Gi1/0/20, Gi1/0/21, Gi1/0/22
                                                Gi1/0/23, Gi1/0/24, Gi1/0/25
                                                Gi1/0/26, Gi1/0/27, Gi1/0/28
                                                Gi1/0/29, Gi1/0/30, Gi1/0/31
                                                Gi1/0/32, Gi1/0/33, Gi1/0/34
                                                Gi1/0/35, Gi1/0/36, Gi1/0/37
                                                Gi1/0/38, Gi1/0/39, Gi1/0/40
                                                Gi1/0/41, Gi1/0/42, Gi1/0/43
                                                Gi1/0/44, Gi1/0/45, Gi1/0/46
                                                Gi1/0/47, Gi1/0/48
2    VLAN0002                         active
40   vlan-40                          active
300  VLAN0300                         active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
2    enet  100002     1500  -      -      -        -    -        0      0
40   enet  100040     1500  -      -      -        -    -        0      0
300  enet  100300     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0
2000 enet  102000     1500  -      -      -        -    -        0      0
3000 enet  103000     1500  -      -      -        -    -        0      0

Remote SPAN VLANs
------------------------------------------------------------------------------
2000,3000

Primary Secondary Type              Ports
```

```
------- --------- ----------------- ----------------------------------------
```

Table 158: show vlan Command Output Fields

Field	Description
VLAN	VLAN number.
Name	Name, if configured, of the VLAN.
Status	Status of the VLAN (active or suspend).
Ports	Ports that belong to the VLAN.
Type	Media type of the VLAN.
SAID	Security association ID value for the VLAN.
MTU	Maximum transmission unit size for the VLAN.
Parent	Parent VLAN, if one exists.
RingNo	Ring number for the VLAN, if applicable.
BrdgNo	Bridge number for the VLAN, if applicable.
Stp	Spanning Tree Protocol type used on the VLAN.
BrdgMode	Bridging mode for this VLAN—possible values are source-route bridging (SRB) and source-route transparent (SRT); the default is SRB.
Trans1	Translation bridge 1.
Trans2	Translation bridge 2.
Remote SPAN VLANs	Identifies any RSPAN VLANs that have been configured.

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 whether the VTP password is configured or not (available in privileged EXEC mode only).
status	Displays general information about the VTP management domain status.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.
Cisco IOS XE Gibraltar 16.12.4	The **show vtp password** command output now displays the password is or is not configured.

Examples

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.
VTP Database Conf Device ID      Primary Server Revision   System Name
             lict
------------ ---- --------------- -------------- ---------- ----------------------
VLAN         Yes  00b0.8e50.d000 000c.0412.6300 12354      main.cisco.com
MST          No   00b0.8e50.d000 0004.AB45.6000 24         main.cisco.com
VLAN         Yes  000c.0412.6300=000c.0412.6300 67         qwerty.cisco.com
```

This is an example of output from the **show vtp counters** command. The table that follows describes each field in the display.

```
Device> show vtp counters
VTP statistics:
Summary advertisements received    : 0
Subset advertisements received     : 0
Request advertisements received    : 0
Summary advertisements transmitted : 0
Subset advertisements transmitted  : 0
Request advertisements transmitted : 0
Number of config revision errors   : 0
Number of config digest errors     : 0
Number of V1 summary errors        : 0

VTP pruning statistics:

Trunk            Join Transmitted Join Received    Summary advts received from
                                                   non-pruning-capable device
---------------- ---------------- ---------------- ---------------------------
Gi1/0/47              0                0                0
Gi1/0/48              0                0                0
Gi2/0/1               0                0                0
Gi3/0/2               0                0                0
```

Table 159: show vtp counters Field Descriptions

Field	Description
Summary advertisements received	Number of summary advertisements received by this device on its trunk ports. Summary advertisements contain the management domain name, the configuration revision number, the update timestamp and identity, the authentication checksum, and the number of subset advertisements to follow.
Subset advertisements received	Number of subset advertisements received by this device on its trunk ports. Subset advertisements contain all the information for one or more VLANs.
Request advertisements received	Number of advertisement requests received by this device on its trunk ports. Advertisement requests normally request information on all VLANs. They can also request information on a subset of VLANs.
Summary advertisements transmitted	Number of summary advertisements sent by this device on its trunk ports. Summary advertisements contain the management domain name, the configuration revision number, the update timestamp and identity, the authentication checksum, and the number of subset advertisements to follow.
Subset advertisements transmitted	Number of subset advertisements sent by this device on its trunk ports. Subset advertisements contain all the information for one or more VLANs.

Field	Description
Request advertisements transmitted	Number of advertisement requests sent by this device on its trunk ports. Advertisement requests normally request information on all VLANs. They can also request information on a subset of VLANs.
Number of configuration revision errors	Number of revision errors. Whenever you define a new VLAN, delete an existing one, suspend or resume an existing VLAN, or modify the parameters on an existing VLAN, the configuration revision number of the device increments. Revision errors increment whenever the device receives an advertisement whose revision number matches the revision number of the device, but the MD5 digest values do not match. This error means that the VTP password in the two devices is different or that the devices have different configurations. These errors indicate that the device is filtering incoming advertisements, which causes the VTP database to become unsynchronized across the network.
Number of configuration digest errors	Number of MD5 digest errors. Digest errors increment whenever the MD5 digest in the summary packet and the MD5 digest of the received advertisement calculated by the device do not match. This error usually means that the VTP password in the two devices is different. To solve this problem, make sure the VTP password on all devices is the same. These errors indicate that the device is filtering incoming advertisements, which causes the VTP database to become unsynchronized across the network.
Number of V1 summary errors	Number of Version 1 errors. Version 1 summary errors increment whenever a device in VTP V2 mode receives a VTP Version 1 frame. These errors indicate that at least one neighboring device is either running VTP Version 1 or VTP Version 2 with V2-mode disabled. To solve this problem, change the configuration of the devices in VTP V2-mode to disabled.
Join Transmitted	Number of VTP pruning messages sent on the trunk.

Field	Description
Join Received	Number of VTP pruning messages received on the trunk.
Summary Advts Received from non-pruning-capable device	Number of VTP summary messages received on the trunk from devices that do not support pruning.

This is an example of output from the **show vtp status** command. The table that follows describes each field in the display.

```
Device> show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 1
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 2037.06ce.3580
Configuration last modified by 192.168.1.1 at 10-10-12 04:34:02
Local updater ID is 192.168.1.1 on interface LIIN0 (first layer3 interface found
)

Feature VLAN:
--------------
VTP Operating Mode                : Server
Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 7
Configuration Revision            : 2
MD5 digest                        : 0xA0 0xA1 0xFE 0x4E 0x7E 0x5D 0x97 0x41
                                    0x89 0xB9 0x9B 0x70 0x03 0x61 0xE9 0x27
```

Table 160: show vtp status Field Descriptions

Field	Description
VTP Version capable	Displays the VTP versions that are capable of operating on the device.
VTP Version running	Displays the VTP version operating on the device. By default, the device implements Version 1 but can be set to Version 2.
VTP Domain Name	Name that identifies the administrative domain for the device.
VTP Pruning Mode	Displays whether pruning is enabled or disabled. Enabling pruning on a VTP server enables pruning for the entire management domain. Pruning restricts flooded traffic to those trunk links that the traffic must use to access the appropriate network devices.
VTP Traps Generation	Displays whether VTP traps are sent to a network management station.
Device ID	Displays the MAC address of the local device.

Field	Description
Configuration last modified	Displays the date and time of the last configuration modification. Displays the IP address of the device that caused the configuration change to the database.
VTP Operating Mode	Displays the VTP operating mode, which can be server, client, or transparent. **Server** —A device in VTP server mode is enabled for VTP and sends advertisements. You can configure VLANs on it. The device guarantees that it can recover all the VLAN information in the current VTP database from NVRAM after reboot. By default, every device is a VTP server. **Note** The device automatically changes from VTP server mode to VTP client mode if it detects a failure while writing the configuration to NVRAM and cannot return to server mode until the NVRAM is functioning. **Client**—A device in VTP client mode is enabled for VTP, can send advertisements, but does not have enough nonvolatile storage to store VLAN configurations. You cannot configure VLANs on it. When a VTP client starts up, it does not send VTP advertisements until it receives advertisements to initialize its VLAN database. **Transparent**—A device in VTP transparent mode is disabled for VTP, does not send or learn from advertisements sent by other devices, and cannot affect VLAN configurations on other devices in the network. The device receives VTP advertisements and forwards them on all trunk ports except the one on which the advertisement was received.
Maximum VLANs Supported Locally	Maximum number of VLANs supported locally.
Number of Existing VLANs	Number of existing VLANs.
Configuration Revision	Current configuration revision number on this device.
MD5 Digest	A 16-byte checksum of the VTP configuration.

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

A private-VLAN host or promiscuous port cannot be a Switched Port Analyzer (SPAN) destination port. If you configure a SPAN destination port as a private-VLAN host or promiscuous port, the port becomes inactive.

Do not configure private VLAN on ports with these other features:

- Dynamic-access port VLAN membership
- Dynamic Trunking Protocol (DTP)
- Port Aggregation Protocol (PAgP)
- Link Aggregation Control Protocol (LACP)
- Multicast VLAN Registration (MVR)
- Voice VLAN

While a port is part of the private-VLAN configuration, any EtherChannel configuration for it is inactive

A private-VLAN port cannot be a secure port and should not be configured as a protected port.

For more information about private-VLAN interaction with other features, see the software configuration guide for this release.

We strongly recommend that you enable spanning tree Port Fast and bridge-protocol-data-unit (BPDU) guard on isolated and community host ports to prevent STP loops due to misconfigurations and to speed up STP convergence.

If you configure a port as a private-VLAN host port and you do not configure a valid private-VLAN association by using the **switchport private-vlan host-association** command, the interface becomes inactive.

If you configure a port as a private-VLAN promiscuous port and you do not configure a valid private VLAN mapping by using the**switchport private-vlan mapping** command, the interface becomes inactive.

Examples

This example shows how to configure an interface as a private-VLAN host port and associate it to primary VLAN 20. The interface is a member of secondary isolated VLAN 501 and primary VLAN 20.

```
(config)# interface gigabitethernet2/0/1
(config-if)# switchport mode private-vlan host
 (config-if)# switchport private-vlan host-association 20 501
 (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.

```
(config)# interface gigabitethernet2/0/1
(config-if)# switchport mode private-vlan promiscuous
 (config-if)# switchport private-vlan mapping 20 501-503
 (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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

When voice VLAN is enabled, you can configure the device to send the Cisco Discovery Protocol (CDP) packets to instruct the IP phone how to send data packets from the device attached to the access port on the Cisco IP Phone. You must enable CDP on the device port connected to the Cisco IP Phone to send the configuration to the Cisco IP Phone. (CDP is enabled by default globally and on all device interfaces.)

You should configure voice VLAN on 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

allowed vlan *vlan-list*	Sets the list of allowed VLANs that can receive and send traffic on this interface in tagged format when in trunking mode. See the Usage Guidelines for the *vlan-list* choices.
native vlan *vlan-id*	Sets the native VLAN for sending and receiving untagged traffic when the interface is in IEEE 802.1Q trunking mode. The range is 1 to 4094.
pruning vlan *vlan-list*	Sets the list of VLANs that are eligible for VTP pruning when in trunking mode. See the Usage Guidelines for the *vlan-list* choices.

Command Default

VLAN 1 is the default native VLAN ID on the port.

The default for all VLAN lists is to include all VLANs.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The *vlan-list* format is **all | none | [add | remove | except]** *vlan-atom* [,*vlan-atom...*]:

- **all** specifies all VLANs from 1 to 4094. This is the default. This keyword is not allowed on commands that do not permit all VLANs in the list to be set at the same time.
- **none** specifies an empty list. This keyword is not allowed on commands that require certain VLANs to be set or at least one VLAN to be set.
- **add** adds the defined list of VLANs to those currently set instead of replacing the list. Valid IDs are from 1 to 1005; extended-range VLANs (VLAN IDs greater than 1005) are valid in some cases.

Note You can add extended-range VLANs to the allowed VLAN list, but not to the pruning-eligible VLAN list.

Separate nonconsecutive VLAN IDs with a comma; use a hyphen to designate a range of IDs.

- **remove** removes the defined list of VLANs from those currently set instead of replacing the list. Valid IDs are from 1 to 1005; extended-range VLAN IDs are valid in some cases.

Note You can remove extended-range VLANs from the allowed VLAN list, but you cannot remove them from the pruning-eligible list.

- **except** lists the VLANs that should be calculated by inverting the defined list of VLANs. (VLANs are added except the ones specified.) Valid IDs are from 1 to 1005. Separate nonconsecutive VLAN IDs with a comma; use a hyphen to designate a range of IDs.
- *vlan-atom* is either a single VLAN number from 1 to 4094 or a continuous range of VLANs described by two VLAN numbers, the lesser one first, separated by a hyphen.

Native VLANs:

- All untagged traffic received on an IEEE 802.1Q trunk port is forwarded with the native VLAN configured for the port.
- If a packet has a VLAN ID that is the same as the sending-port native VLAN ID, the packet is sent without a tag; otherwise, the switch sends the packet with a tag.
- The **no** form of the **native vlan** command resets the native mode VLAN to the appropriate default VLAN for the device.

Allowed VLAN:

- To reduce the risk of spanning-tree loops or storms, you can disable VLAN 1 on any individual VLAN trunk port by removing VLAN 1 from the allowed list. When you remove VLAN 1 from a trunk port, the interface continues to send and receive management traffic, for example, Cisco Discovery Protocol (CDP), Port Aggregation Protocol (PAgP), Link Aggregation Control Protocol (LACP), Dynamic Trunking Protocol (DTP), and VLAN Trunking Protocol (VTP) in VLAN 1.
- The **no** form of the **allowed vlan** command resets the list to the default list, which allows all VLANs.

Trunk pruning:

- The pruning-eligible list applies only to trunk ports.
- Each trunk port has its own eligibility list.
- If you do not want a VLAN to be pruned, remove it from the pruning-eligible list. VLANs that are pruning-ineligible receive flooded traffic.
- VLAN 1, VLANs 1002 to 1005, and extended-range VLANs (VLANs 1006 to 4094) cannot be pruned.

Examples

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.

vlan

To add a VLAN and to enter the VLAN configuration mode, use the **vlan** command in global configuration mode. To delete the VLAN, use the **no** form of this command.

vlan *vlan-id*
no vlan *vlan-id*

Syntax Description

vlan-id	ID of the VLAN to be added and configured. The range is 1 to 4094. You can enter a single VLAN ID, a series of VLAN IDs separated by commas, or a range of VLAN IDs separated by hyphens.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

You can use the **vlan** *vlan-id* global configuration command to add normal-range VLANs (VLAN IDs 1 to 1005) or extended-range VLANs (VLAN IDs 1006 to 4094). Configuration information for normal-range VLANs is always saved in the VLAN database, and you can display this information by entering the **show vlan** privileged EXEC command. If the VTP mode is transparent, VLAN configuration information for normal-range VLANs is also saved in the 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 , the configuration is selected as follows:

- If the VTP mode is transparent in the startup configuration and the VLAN database and the VTP domain name from the VLAN database matches that in the startup configuration file, the VLAN database is ignored (cleared), and the VTP and VLAN configurations in the startup configuration file are used. The VLAN database revision number remains unchanged in the VLAN database.
- If the VTP mode or domain name in the startup configuration do not match the VLAN database, the domain name and VTP mode and configuration for VLAN IDs 1 to 1005 use the VLAN database information.

If you enter an invalid VLAN ID, you receive an error message and do not enter VLAN configuration mode.

Entering the **vlan** command with a VLAN ID enables VLAN configuration mode. When you enter the VLAN ID of an existing VLAN, you do not create a new VLAN, but you can modify VLAN parameters for that VLAN. The specified VLANs are added or modified when you exit the VLAN configuration mode. Only the **shutdown** command (for VLANs 1 to 1005) takes effect immediately.

Note Although all commands are visible, the only VLAN configuration command that is supported on extended-range VLANs is **remote-span**. For extended-range VLANs, all other characteristics must remain at the default state.

These configuration commands are available in VLAN configuration mode. The **no** form of each command returns the characteristic to its default state:

- **are** *are-number*—Defines the maximum number of all-routes explorer (ARE) hops for this VLAN. This keyword applies only to TrCRF VLANs. The range is 0 to 13. The default is 7. If no value is entered, 0 is assumed to be the maximum.
- **backupcrf**—Specifies the backup CRF mode. This keyword applies only to TrCRF VLANs.
  - **enable**—Backup CRF mode for this VLAN.
  - **disable**—Backup CRF mode for this VLAN (the default).
- **bridge** {*bridge-number* | **type**}—Specifies the logical distributed source-routing bridge, the bridge that interconnects all logical rings that have this VLAN as a parent VLAN in FDDI-NET, Token Ring-NET, and TrBRF VLANs. The range is 0 to 15. The default bridge number is 0 (no source-routing bridge) for FDDI-NET, TrBRF, and Token Ring-NET VLANs. The **type** keyword applies only to TrCRF VLANs and is one of these:
  - **srb**—Ssource-route bridging
  - **srt**—Source-route transparent) bridging VLAN
- **exit**—Applies changes, increments the VLAN database revision number (VLANs 1 to 1005 only), and exits VLAN configuration mode.
- **media**—Defines the VLAN media type and is one of these:

Note The supports only Ethernet ports. You configure only FDDI and Token Ring media-specific characteristics for VLAN Trunking Protocol (VTP) global advertisements to other . 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 161: Valid Commands and Syntax for Different Media Types

Media Type	Valid Syntax
Ethernet	**name** *vlan-name*, **media ethernet**, **state** {**suspend** | **active**}, **said** *said-value*, **remote-span**, **tb-vlan1** *tb-vlan1-id*, **tb-vlan2** *tb-vlan2-id*

Media Type	Valid Syntax
FDDI	**name** *vlan-name*, **media fddi**, **state** {**suspend | active**}, **said** *said-value*, **ring** *ring-number*, **parent** *parent-vlan-id*, **tb-vlan1** *tb-vlan1-id*, **tb-vlan2** *tb-vlan2-id*
FDDI-NET	**name** *vlan-name*, **media fd-net** , **state** {**suspend | active**}, **said** *said-value*, **bridge** *bridge-number*, **stp type** {**ieee | ibm | auto**}, **tb-vlan1** *tb-vlan1-id*, **tb-vlan2** *tb-vlan2-id* If VTP v2 mode is disabled, do not set the **stp type** to **auto.**
Token Ring	VTP v1 mode is enabled. **name** *vlan-name*, **media tokenring**, **state** {**suspend | active**}, **said** *said-value*, **ring** *ring-number*, **parent** *parent-vlan-id*, **tb-vlan1** *tb-vlan1-id*, **tb-vlan2** *tb-vlan2-id*
Token Ring concentrator relay function (TrCRF)	VTP v2 mode is enabled. **name** *vlan-name*, **media tokenring**, **state** {**suspend | active**}, **said** *said-value*, **ring** *ring-number*, **parent** *parent-vlan-id*, **bridge type** {**srb | srt**}, **are** *are-number*, **ste** *ste-number*, **backupcrf** {**enable | disable**}, **tb-vlan1** *tb-vlan1-id*, **tb-vlan2** *tb-vlan2-id*
Token Ring-NET	VTP v1 mode is enabled. **name** *vlan-name*, **media tr-net**, **state** {**suspend | active**}, **said** *said-value*, **bridge** *bridge-number*, **stp type** {**ieee | ibm**}, **tb-vlan1** *tb-vlan1-id*, **tb-vlan2** *tb-vlan2-id*
Token Ring bridge relay function (TrBRF)	VTP v2 mode is enabled. **name** *vlan-name*, **media tr-net**, **state** {**suspend | active**}, **said** *said-value*, **bridge** *bridge-number*, **stp type** {**ieee | ibm | auto**}, **tb-vlan1** *tb-vlan1-id*, **tb-vlan2** *tb-vlan2-id*

The following table describes the rules for configuring VLANs:

Table 162: VLAN Configuration Rules

Configuration	Rule
VTP v2 mode is enabled, and you are configuring a TrCRF VLAN media type.	Specify a parent VLAN ID of a TrBRF that already exists in the database. Specify a ring number. Do not leave this field blank. Specify unique ring numbers when TrCRF VLANs have the same parent VLAN ID. Only one backup concentrator relay function (CRF) can be enabled.
VTP v2 mode is enabled, and you are configuring VLANs other than TrCRF media type.	Do not specify a backup CRF.
VTP v2 mode is enabled, and you are configuring a TrBRF VLAN media type.	Specify a bridge number. Do not leave this field blank.
VTP v1 mode is enabled.	No VLAN can have an STP type set to auto. This rule applies to Ethernet, FDDI, FDDI-NET, Token Ring, and Token Ring-NET VLANs.
Add a VLAN that requires translational bridging (values are not set to zero).	The translational bridging VLAN IDs that are used must already exist in the database. The translational bridging VLAN IDs that a configuration points to must also contain a pointer to the original VLAN in one of the translational bridging parameters (for example, Ethernet points to FDDI, and FDDI points to Ethernet). The translational bridging VLAN IDs that a configuration points to must be different media types than the original VLAN (for example, Ethernet can point to Token Ring). If both translational bridging VLAN IDs are configured, these VLANs must be different media types (for example, Ethernet can point to FDDI and Token Ring).

Examples

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:

```
(config)# vlan 200
(config-vlan)# exit
```

```
(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 startup configuration file:

```
(config)# vlan 2000
(config-vlan)# end
# copy running-config startup config
```

You can verify your setting by entering the **show vlan** privileged EXEC command.

vlan dot1q tag native

To enable tagging of native VLAN frames on all IEEE 802.1Q trunk ports, use the **vlan dot1q tag native** command in global configuration mode. To return to the default setting, use the **no** form of this command.

vlan dot1q tag native
no vlan dot1q tag native

Syntax Description

This command has no arguments or keywords.

Command Default

The IEEE 802.1Q native VLAN tagging is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

When enabled, native VLAN packets going out of all IEEE 802.1Q trunk ports are tagged.

When disabled, native VLAN packets going out of all IEEE 802.1Q trunk ports are not tagged.

For more information about IEEE 802.1Q tunneling, see the software configuration guide for this release.

Examples

This example shows how to enable IEEE 802.1Q tagging on native VLAN frames:

```
Device# configure terminal
Device (config)# vlan dot1q tag native
Device (config)# end
```

You can verify your settings by entering the **show vlan dot1q tag native** privileged EXEC command.

vtp (global configuration)

To set or modify the VLAN Trunking Protocol (VTP) configuration characteristics, use the **vtp** command in global configuration mode. To remove the settings or to return to the default settings, use the **no** form of this command.

vtp {**domain** *domain-name* | **file** *filename* | **interface** *interface-name* [**only**] | **mode** {**client** | **off** | **server** | **transparent**} [{**mst** | **unknown** | **vlan**}] | **password** *password* [{**hidden** | **secret**}] | **pruning** | **version** *number*}
no vtp {**file** | **interface** | **mode** [{**client** | **off** | **server** | **transparent**}] [{**mst** | **unknown** | **vlan**}] | **password** | **pruning** | **version**}

Syntax Description

domain *domain-name*	Specifies the VTP domain name, an ASCII string from 1 to 32 characters that identifies the VTP administrative domain for the device. The domain name is case sensitive.
file *filename*	Specifies the Cisco IOS file system file where the VTP VLAN configuration is stored.
interface *interface-name*	Specifies the name of the interface providing the VTP ID updated for this device.
only	(Optional) Uses only the IP address of this interface as the VTP IP updater.
mode	Specifies the VTP device mode as client, server, or transparent.
client	Places the device in VTP client mode. A device in VTP client mode is enabled for VTP, and can send advertisements, but does not have enough nonvolatile storage to store VLAN configurations. You cannot configure VLANs on a VTP client. VLANs are configured on another device in the domain that is in server mode. When a VTP client starts up, it does not send VTP advertisements until it receives advertisements to initialize its VLAN database.
off	Places the device in VTP off mode. A device in VTP off mode functions the same as a VTP transparent device except that it does not forward VTP advertisements on trunk ports.
server	Places the device in VTP server mode. A device in VTP server mode is enabled for VTP and sends advertisements. You can configure VLANs on the device. The device can recover all the VLAN information in the current VTP database from nonvolatile storage after reboot.
transparent	Places the device in VTP transparent mode. A device in VTP transparent mode is disabled for VTP, does not send advertisements or learn from advertisements sent by other devices, and cannot affect VLAN configurations on other devices in the network. The device receives VTP advertisements and forwards them on all trunk ports except the one on which the advertisement was received. When VTP mode is transparent, the mode and domain name are saved in the device running configuration file, and you can save them in the device startup configuration file by entering the **copy running-config startup config** privileged EXEC command.
mst	(Optional) Sets the mode for the multiple spanning tree (MST) VTP database (only VTP Version 3).

unknown	(Optional) Sets the mode for unknown VTP databases (only VTP Version 3).
vlan	(Optional) Sets the mode for VLAN VTP databases. This is the default (only VTP Version 3).
password *password*	Sets the administrative domain password for the generation of the 16-byte secret value used in MD5 digest calculation to be sent in VTP advertisements and to validate received VTP advertisements. The password can be an ASCII string from 1 to 32 characters. The password is case sensitive.
hidden	(Optional) Specifies that the key generated from the password string is saved in the VLAN database file. When the **hidden** keyword is not specified, the password string is saved in clear text. When the hidden password is entered, you need to reenter the password to issue a command in the domain. This keyword is supported only in VTP Version 3.
secret	(Optional) Allows the user to directly configure the password secret key (only VTP Version 3).
pruning	Enables VTP pruning on the device.
version *number*	Sets the VTP Version to Version 1, Version 2, or Version 3.

Command Default

The default filename is *flash:vlan.dat*.

The default mode is server mode and the default database is VLAN.

In VTP Version 3, for the MST database, the default mode is transparent.

No domain name or password is defined.

No password is configured.

Pruning is disabled.

The default version is Version 1.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

When you save VTP mode, domain name, and VLAN configurations in the device startup configuration file and reboot the device, the VTP and VLAN configurations are selected by these conditions:

- If the VTP mode is transparent in the startup configuration and the VLAN database and the VTP domain name from the VLAN database matches that in the startup configuration file, the VLAN database is ignored (cleared), and the VTP and VLAN configurations in the startup configuration file are used. The VLAN database revision number remains unchanged in the VLAN database.
- If the VTP mode or domain name in the startup configuration do not match the VLAN database, the domain name and VTP mode and configuration for VLAN IDs 1 to 1005 use the VLAN database information.

The **vtp file** *filename* cannot be used to load a new database; it renames only the file in which the existing database is stored.

Follow these guidelines when configuring a VTP domain name:

- The device is in the no-management-domain state until you configure a domain name. While in the no-management-domain state, the device does not send any VTP advertisements even if changes occur to the local VLAN configuration. The device leaves the no-management-domain state after it receives the first VTP summary packet on any port that is trunking or after you configure a domain name by using the **vtp domain** command. If the device receives its domain from a summary packet, it resets its configuration revision number to 0. After the device leaves the no-management-domain state, it cannot be configured to reenter it until you clear the NVRAM and reload the software.
- Domain names are case-sensitive.
- After you configure a domain name, it cannot be removed. You can only reassign it to a different domain.

Follow these guidelines when setting VTP mode:

- The **no vtp mode** command returns the device to VTP server mode.
- The **vtp mode server** command is the same as **no vtp mode** except that it does not return an error if the device is not in client or transparent mode.
- If the receiving device is in client mode, the client device changes its configuration to duplicate the configuration of the server. If you have devices in client mode, be sure to make all VTP or VLAN configuration changes on a device in server mode, as it has a higher VTP configuration revision number. If the receiving device is in transparent mode, the device configuration is not changed.
- A device in transparent mode does not participate in VTP. If you make VTP or VLAN configuration changes on a device in transparent mode, the changes are not propagated to other devices in the network.
- If you change the VTP or VLAN configuration on a device that is in server mode, that change is propagated to all the devices in the same VTP domain.
- The **vtp mode transparent** command disables VTP from the domain but does not remove the domain from the device.
- In VTP Versions 1 and 2, the VTP mode must be transparent for VTP and VLAN information to be saved in the running configuration file.
- With VTP Versions 1 and 2, you cannot change the VTP mode to client or server if extended-range VLANs are configured on the switch. Changing the VTP mode is allowed with extended VLANs in VTP Version 3.
- The VTP mode must be transparent for you to add extended-range VLANs or for VTP and VLAN information to be saved in the running configuration file.
- VTP can be set to either server or client mode only when dynamic VLAN creation is disabled.
- The **vtp mode off** command sets the device to off. The **no vtp mode off** command resets the device to the VTP server mode.

Follow these guidelines when setting a VTP password:

- Passwords are case sensitive. Passwords should match on all devices in the same domain.
- When you use the **no vtp password** form of the command, the device returns to the no-password state.

- The **hidden** and **secret** keywords are supported only in VTP Version 3. If you convert from VTP Version 2 to VTP Version 3, you must remove the hidden or secret keyword before the conversion.

Follow these guidelines when setting VTP pruning:

- VTP pruning removes information about each pruning-eligible VLAN from VTP updates if there are no stations belonging to that VLAN.
- If you enable pruning on the VTP server, it is enabled for the entire management domain for VLAN IDs 1 to 1005.
- Only VLANs in the pruning-eligible list can be pruned.
- Pruning is supported with VTP Version 1 and Version 2.

Follow these guidelines when setting the VTP version:

- Toggling the Version 2 (v2) mode state modifies parameters of certain default VLANs.
- Each VTP device automatically detects the capabilities of all the other VTP devices. To use Version 2, all VTP devices in the network must support Version 2; otherwise, you must configure them to operate in VTP Version 1 mode.
- If all devices in a domain are VTP Version 2-capable, you only need to configure Version 2 on one device; the version number is then propagated to the other Version-2 capable devices in the VTP domain.
- If you are using VTP in a Token Ring environment, VTP Version 2 must be enabled.
- If you are configuring a Token Ring bridge relay function (TrBRF) or Token Ring concentrator relay function (TrCRF) VLAN media type, you must use Version 2.
- If you are configuring a Token Ring or Token Ring-NET VLAN media type, you must use Version 1.
- In VTP Version 3, all database VTP information is propagated across the VTP domain, not only VLAN database information.
- Two VTP Version 3 regions can only communicate over a VTP Version 1 or VTP Version 2 region in transparent mode.

You cannot save password, pruning, and version configurations in the device configuration file.

Examples

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

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Enter this command only on interfaces that are in trunking mode.

Examples

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

mst	(Optional) Configures the device as the primary VTP server for the multiple spanning tree (MST) feature.
vlan	(Optional) Configures the device as the primary VTP server for VLANs.
force	(Optional) Configures the device to not check for conflicting devices when configuring the primary server.

Command Default

The device is a VTP secondary server.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

A VTP primary server updates the database information and sends updates that are honored by all devices in the system. A VTP secondary server can only back up the updated VTP configurations received from the primary server to NVRAM.

By default, all devices come up as secondary servers. Primary server status is needed only for database updates when the administrator issues a takeover message in the domain. You can have a working VTP domain without any primary servers.

Primary server status is lost if the device reloads or domain parameters change.

Note This command is supported only when the device is running VTP Version 3.

Examples

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.