



Command Reference, Cisco IOS XE Fuji 16.9.x (Catalyst 9400 Switches)

First Published: 2018-07-18

Last Modified: 2018-09-28

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

© 2018 Cisco Systems, Inc. All rights reserved.

CONTENTS

CHAPTER 1

Using the Command-Line Interface	1
Using the Command-Line Interface	1
Understanding Command Modes	1
Understanding the Help System	3
Understanding Abbreviated Commands	3
Understanding no and default Forms of Commands	4
Understanding CLI Error Messages	4
Using Configuration Logging	4
Using Command History	5
Changing the Command History Buffer Size	5
Recalling Commands	5
Disabling the Command History Feature	6
Using Editing Features	6
Enabling and Disabling Editing Features	6
Editing Commands through Keystrokes	6
Editing Command Lines that Wrap	8
Searching and Filtering Output of show and more Commands	9
Accessing the CLI	9
Accessing the CLI through a Console Connection or through Telnet	10

PART I

Cisco SD-Access	11
------------------------	-----------

CHAPTER 2

Campus Fabric Commands	13
broadcast-underlay	14
database-mapping	14
dynamic-eid	16

eid-record-provider	17
eid-record-subscriber	17
eid-table	18
encapsulation	19
etr	20
etr map-server	21
extranet	22
instance-id	22
ip pim lisp core-group-range	23
ip pim lisp transport multicast	23
ip pim rp-address	24
ip pim sparse mode	25
ipv4 multicast multitopology	25
ip pim ssm	26
itr	27
itr map-resolver	27
locator default-set	28
locator-set	29
map-cache	29
map-cache extranet	30
prefix-list	30
route-import database	31
service	32
show lisp instance-id ipv4 database	33
show lisp instance-id ipv6 database	34
show lisp instance-id ipv4 map-cache	35
show lisp instance-id ipv6 map-cache	40
show lisp instance-id ipv4 server	42
show lisp instance-id ipv6 server	44
show lisp instance-id ipv4 statistics	44
show lisp instance-id ipv6 statistics	45
show lisp prefix-list	45
show lisp session	46
use-petr	47

PART II**High Availability 49**

CHAPTER 3**High Availability Commands 51**

main-cpu 51
mode sso 52
policy config-sync prc reload 52
redundancy 53
redundancy reload peer 54
redundancy reload shelf 55
reload 55
show redundancy 57
show redundancy config-sync 60
standby console enable 62

CHAPTER 4**Graceful Insertion and Removal 65**

maintenance-template 65
router routing protocol shutdown l2 66
start maintenance 66
stop maintenance 67
system mode maintenance 67

CHAPTER 5**Cisco StackWise Virtual Commands 69**

clear diagnostic event-log 69
stackwise-virtual 70
diagnostic monitor 71
diagnostic schedule module 72
diagnostic start 75
diagnostic stop 77
domain id 78
dual-active detection pagp 79
hw-module beacon switch 79
hw-module switch slot 80
hw-module switch usbflash 82

stackwise-virtual link	82
stackwise-virtual dual-active-detection	83
show hw-module switch subslot	83
show logging onboard switch	85
show stackwise-virtual	88

PART III**Interface and Hardware Components** **91**

CHAPTER 6**Interface and Hardware Commands** **93**

debug ilpower	94
debug interface	95
debug lldp packets	96
debug platform poe	96
duplex	97
errdisable detect cause	98
errdisable recovery cause	100
errdisable recovery interval	102
hw-module beacon	103
hw-module subslot mode	104
interface	105
interface range	107
lldp (interface configuration)	108
logging event power-inline-status	109
mode (power-stack configuration)	110
network-policy	111
network-policy profile (global configuration)	112
power efficient-ethernet auto	113
power-priority	114
power inline	115
power inline police	117
power supply	119
show beacon all	120
show eee	122
show env	124

show errdisable detect **126**
show errdisable recovery **127**
show hardware led **127**
show hw-module subslot mode **130**
show idprom fan-tray **131**
show ip interface **131**
show interfaces **136**
show interfaces counters **139**
show interfaces switchport **141**
show interfaces transceiver **143**
show inventory **145**
show log onboard slot **147**
show memory platform **148**
show module **150**
show mgmt-infra trace messages ilpower **150**
show mgmt-infra trace messages ilpower-ha **152**
show mgmt-infra trace messages platform-mgr-poe **152**
show network-policy profile **153**
show platform hardware fed active forward **154**
show platform hardware iomd lc-portmap brief **155**
show platform hardware iomd portgroups **156**
show platform resources **157**
show platform software ilpower **157**
show platform software process list **159**
show platform software process slot switch **162**
show platform software status control-processor **163**
show processes cpu platform monitor **166**
show processes memory platform **167**
show system mtu **170**
show tech-support **170**
speed **172**
switchport block **173**
system mtu **174**
voice-signaling vlan (network-policy configuration) **175**

voice vlan (network-policy configuration) 176

PART IV

IP Addressing Services 179

CHAPTER 7

IP Addressing Services Commands 181

clear ip nhrp 181
debug nhrp 182
fhrp delay 184
fhrp version vrrp v3 185
ip address 185
ip address dhcp 188
ip address pool (DHCP) 190
ip nhrp map 191
ip nhrp map multicast 192
ip nhrp network-id 193
ip nhrp nhs 194
ipv6 nd cache expire 196
ipv6 nd na glean 197
ipv6 nd nud retry 197
key chain 199
key-string (authentication) 200
key 201
show ip nhrp nhs 201
show ip ports all 203
show key chain 205
show track 205
track 207
vrrp 208
vrrp description 209
vrrp preempt 210
vrrp priority 211
vrrp timers advertise 211
vrrs leader 212

PART V**IP Multicast Routing 215**

CHAPTER 8**IP Multicast Routing Commands 217**

- clear ip igmp snooping membership 218
- clear ip mfib counters 218
- clear ip mroute 219
- clear ip pim snooping vlan 220
- ip igmp filter 221
- ip igmp max-groups 222
- ip igmp profile 223
- ip igmp snooping 224
- ip igmp snooping last-member-query-count 225
- ip igmp snooping querier 226
- ip igmp snooping report-suppression 228
- ip igmp snooping vlan explicit-tracking 229
- ip igmp snooping vlan mrouter 230
- ip igmp snooping vlan static 230
- ip multicast auto-enable 231
- ip pim accept-register 232
- ip pim bsr-candidate 233
- ip pim rp-candidate 234
- ip pim send-rp-announce 235
- ip pim snooping 236
- ip pim snooping dr-flood 237
- ip pim snooping vlan 238
- ip pim spt-threshold 239
- match message-type 239
- match service-type 240
- match service-instance 241
- mrinfo 241
- service-policy-query 242
- service-policy 243
- show ip igmp filter 244

show ip igmp profile	244
show ip igmp snooping	245
show ip igmp snooping groups	247
show ip igmp snooping membership	248
show ip igmp snooping mrouter	250
show ip igmp snooping querier	250
show ip pim autorp	252
show ip pim bsr-router	253
show ip pim bsr	253
show ip pim snooping	254
show ip pim tunnel	257
show platform software fed switch ip multicast	258

PART VI**IPv6** 261

CHAPTER 9**IPv6 Commands** 263

clear ipv6 access-list	266
clear ipv6 dhcp	267
clear ipv6 dhcp binding	267
clear ipv6 dhcp client	268
clear ipv6 dhcp conflict	269
clear ipv6 dhcp relay binding	270
clear ipv6 eigrp	271
clear ipv6 mfib counters	271
clear ipv6 mld counters	272
clear ipv6 mld traffic	273
clear ipv6 mtu	273
clear ipv6 multicast aaa authorization	274
clear ipv6 nd destination	275
clear ipv6 nd on-link prefix	275
clear ipv6 nd router	276
clear ipv6 neighbors	277
clear ipv6 nhrp	278
clear ipv6 ospf	279

clear ipv6 ospf counters	280
clear ipv6 ospf events	281
clear ipv6 pim reset	282
clear ipv6 pim topology	282
clear ipv6 pim traffic	283
clear ipv6 prefix-list	283
clear ipv6 rip	284
clear ipv6 route	285
clear ipv6 spd	286
clear ipv6 traffic	287
ipv6 access-list	288
ipv6 cef	291
ipv6 cef accounting	292
ipv6 cef distributed	294
ipv6 cef load-sharing algorithm	295
ipv6 cef optimize neighbor resolution	296
ipv6 destination-guard policy	297
ipv6 dhcp-relay bulk-lease	297
ipv6 dhcp-relay option vpn	298
ipv6 dhcp-relay source-interface	299
ipv6 dhcp binding track ppp	300
ipv6 dhcp database	301
ipv6 dhcp iana-route-add	302
ipv6 dhcp iapd-route-add	303
ipv6 dhcp-ldra	303
ipv6 dhcp ping packets	304
ipv6 dhcp pool	305
ipv6 flow monitor	307
ipv6 dhcp server vrf enable	308
ipv6 general-prefix	308
ipv6 local policy route-map	310
ipv6 local pool	311
ipv6 mld snooping	312
ipv6 mld ssm-map enable	313

ipv6 mld state-limit	314
ipv6 multicast-routing	315
ipv6 multicast group-range	316
ipv6 multicast pim-passive-enable	317
ipv6 multicast rpf	318
ipv6 nd cache expire	319
ipv6 nd cache interface-limit (global)	319
ipv6 nd host mode strict	320
ipv6 nd ns-interval	321
ipv6 nd reachable-time	322
ipv6 nd resolution data limit	323
ipv6 nd route-owner	324
ipv6 neighbor	325
ipv6 ospf name-lookup	326
ipv6 pim	327
ipv6 pim accept-register	328
ipv6 pim allow-rp	328
ipv6 pim anycast-RP	329
ipv6 pim neighbor-filter list	330
ipv6 pim rp-address	331
ipv6 pim rp embedded	333
ipv6 pim spt-threshold infinity	334
ipv6 prefix-list	334
ipv6 source-guard attach-policy	337
ipv6 source-route	338
ipv6 spd mode	339
ipv6 spd queue max-threshold	340
ipv6 traffic interface-statistics	341
ipv6 unicast-routing	341
show ipv6 access-list	342
show ipv6 destination-guard policy	344
show ipv6 dhcp	345
show ipv6 dhcp binding	346
show ipv6 dhcp conflict	348

show ipv6 dhcp database **349**
show ipv6 dhcp guard policy **350**
show ipv6 dhcp interface **352**
show ipv6 dhcp relay binding **354**
show ipv6 eigrp events **355**
show ipv6 eigrp interfaces **356**
show ipv6 eigrp topology **358**
show ipv6 eigrp traffic **360**
show ipv6 general-prefix **361**
show ipv6 interface **362**
show ipv6 mfib **369**
show ipv6 mld groups **375**
show ipv6 mld interface **377**
show ipv6 mld snooping **379**
show ipv6 mld ssm-map **380**
show ipv6 mld traffic **382**
show ipv6 mrib client **383**
show ipv6 mrib route **384**
show ipv6 mroute **386**
show ipv6 mtu **390**
show ipv6 nd destination **391**
show ipv6 nd on-link prefix **392**
show ipv6 neighbors **393**
show ipv6 nhrp **396**
show ipv6 ospf **399**
show ipv6 ospf border-routers **403**
show ipv6 ospf event **404**
show ipv6 ospf graceful-restart **406**
show ipv6 ospf interface **407**
show ipv6 ospf request-list **412**
show ipv6 ospf retransmission-list **413**
show ipv6 ospf statistics **414**
show ipv6 ospf summary-prefix **416**
show ipv6 ospf timers rate-limit **417**

show ipv6 ospf traffic **418**
show ipv6 ospf virtual-links **421**
show ipv6 pim anycast-RP **423**
show ipv6 pim bsr **423**
show ipv6 pim df **425**
show ipv6 pim group-map **427**
show ipv6 pim interface **429**
show ipv6 pim join-prune statistic **430**
show ipv6 pim limit **431**
show ipv6 pim neighbor **432**
show ipv6 pim range-list **433**
show ipv6 pim topology **434**
show ipv6 pim traffic **436**
show ipv6 pim tunnel **438**
show ipv6 policy **439**
show ipv6 prefix-list **440**
show ipv6 protocols **442**
show ipv6 rip **445**
show ipv6 route **450**
show ipv6 routers **453**
show ipv6 rpf **456**
show ipv6 source-guard policy **458**
show ipv6 spd **458**
show ipv6 static **459**
show ipv6 traffic **462**
show ipv6 pim tunnel **465**

PART VII

Layer 2/3 **467**

CHAPTER 10

Layer 2/3 Commands **469**

channel-group **470**
channel-protocol **473**
clear lacp **474**
clear pagp **474**

clear spanning-tree counters **475**
clear spanning-tree detected-protocols **476**
debug etherchannel **476**
debug lacp **477**
debug pagp **478**
debug platform pm **479**
debug platform udld **480**
debug spanning-tree **480**
interface port-channel **482**
lacp max-bundle **483**
lacp port-priority **484**
lacp rate **485**
lacp system-priority **485**
pagp learn-method **486**
pagp port-priority **487**
port-channel **488**
port-channel auto **489**
port-channel load-balance **489**
port-channel load-balance extended **490**
port-channel min-links **491**
rep admin vlan **492**
rep block port **493**
rep lsl-age-timer **494**
rep lsl-retries **495**
rep preempt delay **495**
rep preempt segment **496**
rep segment **497**
rep stcn **499**
show etherchannel **500**
show interfaces rep detail **502**
show lacp **503**
show pagp **507**
show platform etherchannel **508**
show platform pm **509**

show rep topology	509
show udld	511
switchport	514
switchport access vlan	515
switchport mode	515
switchport nonegotiate	517
switchport voice vlan	518
udld	521
udld port	522
udld reset	523

PART VIII**Multiprotocol Label Switching** 525**CHAPTER 11****MPLS Commands** 527

mpls ip default-route	527
mpls ip (global configuration)	528
mpls ip (interface configuration)	529
mpls label protocol (global configuration)	530
mpls label protocol (interface configuration)	530
mpls label range	531
mpls static binding ipv4	533
show mpls forwarding-table	535
show mpls label range	542
show mpls static binding	542
show mpls static crossconnect	544

CHAPTER 12**Multicast VPN Commands** 547

ip multicast-routing	547
ip multicast mrinfo-filter	548
mdt data	549
mdt default	550
mdt log-reuse	551
show ip pim mdt bgp	552
show ip pim mdt history	553

show ip pim mdt receive 554

show ip pim mdt send 555

PART IX Network Management 557

CHAPTER 13 Encrypted Traffic Analytics 559

et-analytics 559

et-analytics enable 560

inactive time 560

ip flow-export destination 561

show flow monitor etta-mon cache 562

show platform software et-analytics 562

show platform software fed switch active fnf et-analytics-flow-dump 563

CHAPTER 14 Network Management Commands 565

description (ERSPAN) 566

destination (ERSPAN) 567

erspan-id 568

event manager applet 569

filter (ERSPAN) 572

ip ttl (ERSPAN) 573

ip wccp 574

monitor capture (interface/control plane) 575

monitor capture buffer 577

monitor capture clear 578

monitor capture export 578

monitor capture file 579

monitor capture limit 580

monitor capture match 581

monitor capture start 582

monitor capture stop 582

monitor session 583

monitor session destination 584

monitor session filter 588

monitor session source	589
monitor session type erspan-source	591
origin	592
show ip sla statistics	593
show capability feature monitor	594
show monitor	595
show monitor capture	597
show monitor session	598
show platform software fed switch ip wccp	600
show platform software swspan	602
snmp ifmib ifindex persist	603
snmp-server enable traps	604
snmp-server enable traps bridge	606
snmp-server enable traps bulkstat	607
snmp-server enable traps call-home	608
snmp-server enable traps cef	609
snmp-server enable traps cpu	609
snmp-server enable traps envmon	610
snmp-server enable traps errdisable	611
snmp-server enable traps flash	612
snmp-server enable traps isis	613
snmp-server enable traps license	613
snmp-server enable traps mac-notification	614
snmp-server enable traps ospf	615
snmp-server enable traps pim	616
snmp-server enable traps port-security	617
snmp-server enable traps power-ethernet	618
snmp-server enable traps snmp	618
snmp-server enable traps storm-control	619
snmp-server enable traps stpx	620
snmp-server enable traps transceiver	621
snmp-server enable traps vrfmib	621
snmp-server enable traps vstack	622
snmp-server engineID	623

snmp-server host **624**
source (ERSPAN) **628**
switchport mode access **629**
switchport voice vlan **629**

CHAPTER 15 Flexible NetFlow Commands **631**

cache **632**
clear flow exporter **634**
clear flow monitor **635**
collect **636**
collect counter **637**
collect interface **637**
collect timestamp absolute **638**
collect transport tcp flags **639**
datalink flow monitor **640**
debug flow exporter **641**
debug flow monitor **641**
debug flow record **642**
debug sampler **643**
description **643**
destination **644**
dscp **645**
export-protocol netflow-v9 **645**
export-protocol netflow-v5 **646**
exporter **646**
flow exporter **647**
flow monitor **647**
flow record **648**
ip flow monitor **649**
ipv6 flow monitor **650**
match datalink ethertype **651**
match datalink mac **652**
match datalink vlan **653**
match flow cts **654**

match flow direction	654
match interface	655
match ipv4	656
match ipv4 destination address	657
match ipv4 source address	657
match ipv4 ttl	658
match ipv6	658
match ipv6 destination address	659
match ipv6 hop-limit	660
match ipv6 source address	660
match transport	661
match transport icmp ipv4	662
match transport icmp ipv6	662
mode random 1 out-of	663
option	664
record	665
sampler	666
show flow exporter	666
show flow interface	668
show flow monitor	669
show flow record	671
show sampler	672
source	673
template data timeout	674
transport	675
ttl	676

PART X

QoS 677

CHAPTER 16

Auto QoS Commands 679

auto qos classify	679
auto qos trust	681
auto qos video	688
auto qos voip	697

debug auto qos **710**
show auto qos **711**

CHAPTER 17 QoS Commands **713**

class **713**
class-map **715**
match (class-map configuration) **717**
policy-map **719**
priority **721**
queue-buffers ratio **723**
queue-limit **724**
random-detect cos **725**
random-detect cos-based **726**
random-detect dscp **727**
random-detect dscp-based **728**
random-detect precedence **729**
random-detect precedence-based **731**
service-policy (Wired) **732**
set **733**
show class-map **738**
show platform hardware fed active qos **739**
show platform software fed switch qos **742**
show platform software fed switch qos qsb **743**
show policy-map **745**
trust device **747**

PART XI Routing **749**

CHAPTER 18 Bidirectional Forwarding Detection Commands **751**

authentication (BFD) **751**
bfd **752**
bfd all-interfaces **753**
bfd check-ctrl-plane-failure **754**
bfd echo **755**

bfd slow-timers	756
bfd template	757
bfd-template single-hop	757
ip route static bfd	758
ipv6 route static bfd	760

CHAPTER 19

IP Routing Commands	763
aggregate-address	764
area nssa	767
area virtual-link	768
auto-summary (BGP)	771
bgp graceful-restart	773
clear proximity ip bgp	775
default-information originate (OSPF)	779
default-metric (BGP)	780
distance (OSPF)	782
eigrp log-neighbor-changes	784
ip authentication key-chain eigrp	785
ip authentication mode eigrp	786
ip bandwidth-percent eigrp	787
ip cef load-sharing algorithm	788
ip community-list	789
ip prefix-list	793
ip hello-interval eigrp	796
ip hold-time eigrp	797
ip load-sharing	798
ip ospf database-filter all out	799
ip ospf name-lookup	800
ip split-horizon eigrp	800
ip summary-address eigrp	801
metric weights (EIGRP)	803
neighbor advertisement-interval	805
neighbor default-originate	806
neighbor description	808

neighbor ebgp-multihop **809**
neighbor maximum-prefix (BGP) **810**
neighbor peer-group (assigning members) **812**
neighbor peer-group (creating) **813**
neighbor route-map **816**
neighbor update-source **817**
network (BGP and multiprotocol BGP) **819**
network (EIGRP) **821**
nsf (EIGRP) **822**
offset-list (EIGRP) **823**
redistribute (IP) **824**
router-id **832**
router bgp **833**
router eigrp **836**
router ospf **836**
set community **837**
set ip next-hop (BGP) **839**
show ip bgp **841**
show ip bgp neighbors **852**
show ip eigrp interfaces **871**
show ip eigrp neighbors **874**
show ip eigrp topology **876**
show ip eigrp traffic **881**
show ip ospf **882**
show ip ospf border-routers **889**
show ip ospf database **890**
show ip ospf interface **899**
show ip ospf neighbor **902**
show ip ospf virtual-links **907**
summary-address (OSPF) **908**
timers throttle spf **909**

CHAPTER 20**Security** 913

aaa accounting	915
aaa accounting dot1x	918
aaa accounting identity	919
aaa authentication dot1x	920
aaa new-model	921
authentication host-mode	922
authentication mac-move permit	924
authentication priority	924
authentication violation	927
cisp enable	928
clear errdisable interface vlan	929
clear mac address-table	930
confidentiality-offset	931
cts manual	932
cts role-based enforcement	933
cts role-based l2-vrf	934
cts role-based monitor	936
cts role-based permissions	937
delay-protection	938
deny (MAC access-list configuration)	939
device-role (IPv6 snooping)	942
device-role (IPv6 nd inspection)	942
device-tracking policy	943
dot1x critical (global configuration)	944
dot1x pae	945
dot1x supplicant controlled transient	946
dot1x supplicant force-multicast	946
dot1x test eapol-capable	947
dot1x test timeout	948
dot1x timeout	949
dtls	951
epm access-control open	952

include-icv-indicator	953
ip access-list role-based	954
ip admission	955
ip admission name	955
ip dhcp snooping database	957
ip dhcp snooping information option format remote-id	959
ip dhcp snooping verify no-relay-agent-address	959
ip http access-class	960
ip radius source-interface	961
ip source binding	963
ip verify source	963
ipv6 access-list	964
ipv6 snooping policy	966
key chain macsec	967
key-server	968
limit address-count	969
mab request format attribute 32	970
macsec-cipher-suite	971
macsec network-link	972
match (access-map configuration)	973
mka pre-shared-key	974
mka suppress syslogs sak-rekey	974
authentication logging verbose	975
dot1x logging verbose	976
mab logging verbose	977
permit (MAC access-list configuration)	977
propagate sgt (cts manual)	980
protocol (IPv6 snooping)	982
radius server	982
sak-rekey	984
sap mode-list (cts manual)	985
security level (IPv6 snooping)	987
send-secure-announcements	987
server-private (RADIUS)	988

show aaa clients	990
show aaa command handler	991
show aaa local	991
show aaa servers	992
show aaa sessions	993
show authentication brief	994
show authentication sessions	996
show cts interface	998
show cts role-based permissions	1000
show cisp	1001
show dot1x	1003
show eap pac peer	1004
show ip dhcp snooping statistics	1004
show radius server-group	1007
show vlan access-map	1008
show vlan filter	1009
show vlan group	1009
switchport port-security aging	1010
switchport port-security mac-address	1011
switchport port-security maximum	1013
switchport port-security violation	1014
tacacs server	1016
tracking (IPv6 snooping)	1017
trusted-port	1018
vlan access-map	1019
vlan dot1Q tag native	1021
vlan filter	1021
vlan group	1022

PART XIII**System Management** 1025

CHAPTER 21**System Management Commands** 1027

arp	1028
boot	1029

cat **1030**
copy **1030**
copy startup-config tftp: **1031**
copy tftp: startup-config **1032**
debug voice diagnostics mac-address **1033**
delete **1033**
dir **1034**
exit **1035**
flash_init **1035**
help **1036**
hw-module slot shutdown **1037**
hw-module subslot oir power-cycle **1037**
install **1038**
l2 traceroute **1042**
license boot level **1042**
license smart deregister **1043**
license smart register idtoken **1044**
license smart renew **1045**
location **1046**
location plm calibrating **1049**
mac address-table move update **1049**
mgmt_init **1050**
mkdir **1051**
more **1052**
no debug all **1052**
power budget mode **1053**
rename **1054**
reset **1054**
rmdir **1055**
sdm prefer **1056**
service private-config-encryption **1056**
set **1057**
show cable-diagnostics tdr **1059**
show debug **1061**

show env	1062
show env xps	1066
show flow monitor	1069
show install	1071
show license all	1073
show license status	1075
show license summary	1076
show license udi	1077
show license usage	1077
show location	1078
show mac address-table move update	1079
show parser encrypt file status	1080
show platform integrity	1081
show platform sudi certificate	1082
show sdm prefer	1083
show tech-support license	1084
test cable-diagnostics tdr	1085
traceroute mac	1086
traceroute mac ip	1089
type	1091
unset	1092
version	1093

CHAPTER 22**Tracing** 1095

Information About Tracing	1095
Tracing Overview	1095
Location of Tracelogs	1095
Tracelog Naming Convention	1096
Rotation and Throttling Policy	1096
Tracing Levels	1096
set platform software trace	1097
show platform software trace filter-binary	1101
show platform software trace message	1101
show platform software trace level	1104

request platform software trace archive **1107**
request platform software trace rotate all **1108**
request platform software trace filter-binary **1108**

PART XIV**VLAN 1111****CHAPTER 23****VLAN Commands 1113**

clear vtp counters **1113**
debug platform vlan **1114**
debug sw-vlan **1114**
debug sw-vlan ifs **1115**
debug sw-vlan notification **1116**
debug sw-vlan vtp **1117**
interface vlan **1118**
show platform vlan **1119**
show vlan **1119**
show vtp **1122**
switchport priority extend **1127**
switchport trunk **1128**
vlan **1130**
vtp (global configuration) **1136**
vtp (interface configuration) **1140**
vtp primary **1141**

Notices 1143

CHAPTER ■

Using the Command-Line Interface

This chapter contains the following topics:

- [Using the Command-Line Interface, on page 1](#)

Using the Command-Line Interface

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

Understanding Command Modes

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

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

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

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

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

Table 1: Command Mode Summary

Mode	Access Method	Prompt	Exit Method	About This Mode
User EXEC	Begin a session with your switch.	Switch>	Enter logout or quit .	Use this mode to <ul style="list-style-type: none"> Change terminal settings. Perform basic tests. Display system information.
Privileged EXEC	While in user EXEC mode, enter the enable command.	Device#	Enter disable to exit.	Use this mode to verify commands that you have entered. Use a password to protect access to this mode.
Global configuration	While in privileged EXEC mode, enter the configure command.	Device(config)#	To exit to privileged EXEC mode, enter exit or end , or press Ctrl-Z .	Use this mode to configure parameters that apply to the entire switch.
VLAN configuration	While in global configuration mode, enter the vlan <i>vlan-id</i> command.	Device(config-vlan)#	To exit to global configuration mode, enter the exit command. To return to privileged EXEC mode, press Ctrl-Z or enter end .	Use this mode to configure VLAN parameters. When VTP mode is transparent, you can create extended-range VLANs (VLAN IDs greater than 1005) and save configurations in the switch startup configuration file.
Interface configuration	While in global configuration mode, enter the interface command (with a specific interface).	Device(config-if)#	To exit to global configuration mode, enter exit . To return to privileged EXEC mode, press Ctrl-Z or enter end .	Use this mode to configure parameters for the Ethernet ports.
Line configuration	While in global configuration mode, specify a line with the line vty or line console command.	Device(config-line)#	To exit to global configuration mode, enter exit . To return to privileged EXEC mode, press Ctrl-Z or enter end .	Use this mode to configure parameters for the terminal line.

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

Understanding the Help System

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

Table 2: Help Summary

Command	Purpose
help	Obtains a brief description of the help system in any command mode.
<i>abbreviated-command-entry</i> ? Device# di ? dir disable disconnect	Obtains a list of commands that begin with a particular character string.
<i>abbreviated-command-entry</i> <Tab> Device# sh conf <tab> Device# show configuration	Completes a partial command name.
? Switch> ?	Lists all commands available for a particular command mode.
<i>command</i> ? Switch> show ?	Lists the associated keywords for a command.
<i>command keyword</i> ? Device(config)# cdp holdtime ? <10-255> Length of time (in sec) that receiver must keep this packet	Lists the associated arguments for a keyword.

Understanding Abbreviated Commands

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

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

```
Device# show conf
```

Understanding no and default Forms of Commands

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

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

Understanding CLI Error Messages

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

Table 3: Common CLI Error Messages

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

Using Configuration Logging

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



Note Only CLI or HTTP changes are logged.

Using Command History

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

Changing the Command History Buffer Size

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

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

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

The range is from 0 to 256.

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

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

The range is from 0 to 256.

Recalling Commands

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



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

Table 4: Recalling Commands

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

Disabling the Command History Feature

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

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

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

Using Editing Features

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

Enabling and Disabling Editing Features

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

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

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

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

```
Device# terminal editing
```

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

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

Editing Commands through Keystrokes

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



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

Table 5: Editing Commands through Keystrokes

Capability	Keystroke	Purpose
Move around the command line to make changes or corrections.	Press Ctrl-B , or press the left arrow key.	Moves the cursor back one character.

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

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

Editing Command Lines that Wrap

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

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


Note

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

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

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

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

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

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

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

Searching and Filtering Output of show and more Commands

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

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

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

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

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

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

Accessing the CLI

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

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



Note

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

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

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

Accessing the CLI through a Console Connection or through Telnet

system prompt for the active switch is Switch. Only the **show** and **debug** commands are available in a CLI session to a specific stack member.

Accessing the CLI through a Console Connection or through Telnet

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

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

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

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

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

The switch supports up to five simultaneous secure SSH sessions.

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



PART I

Cisco SD-Access

- [Campus Fabric Commands, on page 13](#)

CHAPTER

Campus Fabric Commands

- broadcast-underlay, on page 14
- database-mapping, on page 14
- dynamic-eid, on page 16
- eid-record-provider, on page 17
- eid-record-subscriber, on page 17
- eid-table, on page 18
- encapsulation, on page 19
- etr, on page 20
- etr map-server, on page 21
- extranet, on page 22
- instance-id, on page 22
- ip pim lisp core-group-range, on page 23
- ip pim lisp transport multicast, on page 23
- ip pim rp-address, on page 24
- ip pim sparse mode, on page 25
- ipv4 multicast multitopology, on page 25
- ip pim ssm, on page 26
- itr, on page 27
- itr map-resolver, on page 27
- locator default-set, on page 28
- locator-set, on page 29
- map-cache , on page 29
- map-cache extranet, on page 30
- prefix-list, on page 30
- route-import database, on page 31
- service, on page 32
- show lisp instance-id ipv4 database, on page 33
- show lisp instance-id ipv6 database, on page 34
- show lisp instance-id ipv4 map-cache, on page 35
- show lisp instance-id ipv6 map-cache, on page 40
- show lisp instance-id ipv4 server, on page 42
- show lisp instance-id ipv6 server, on page 44
- show lisp instance-id ipv4 statistics, on page 44

broadcast-underlay

- [show lisp instance-id ipv6 statistics, on page 45](#)
- [show lisp prefix-list, on page 45](#)
- [show lisp session, on page 46](#)
- [use-petr, on page 47](#)

broadcast-underlay

To configure the underlay in a LISP network to use a multicast 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	<i>multicast-ip</i> 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	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.2</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.2	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.2	This command was introduced.				
Usage Guidelines	<p>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.</p> <p>Use the no form of the command to remove the broadcast functionality.</p>				

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	<i>eid-prefix / prefix-length</i>	Specifies the IPv4 or IPv6 endpoint identifier prefix and length that is advertised by the router.
locator-set <i>RLOC-name</i>		Specifies the routing locator (RLOC) associated with the value specified for the eid-prefix.
proxy		Enables configuration of static proxy database mapping.
ipv4 interface <i>interface-name</i>		Specifies the IPv4 address and name of the interface to be used as the RLOC for the EID prefix.
ipv6 interface <i>interface-name</i>		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 Everest 16.6.2	This command was introduced.
	Cisco IOS XE Fuji 16.9.1	Introduced support for the keyword proxy .
Usage Guidelines	<p>In the LISP-instance-service configuration mode, the database-mapping command configures LISP database parameters a specified IPv4 or IPv6 EID-prefix block. The <i>locator</i> 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.</p> <p>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.</p> <p>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.</p>	
	<p>The following example shows how to map the eid-prefix with the locator-set, RLOC, in the EID configuration mode, on an external border:</p> 	
Note	Ensure that the locator-set RLOC is already configured.	

dynamic-eid

```

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 <i>vrf-name</i>	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	<i>eid-name</i> If <i>eid-name</i> exists, it enters <i>eid-name</i> configuration mode. Else, a new dynamic-eid policy with name <i>eid-name</i> 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	<table> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.2</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.2	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.2	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	<table border="1"> <thead> <tr> <th>Command D</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>lisp mobility</td> <td>Configures an interface on an ITR to participate in LISP mobility (dynamic-EID roaming).</td> </tr> </tbody> </table>	Command D	Description	lisp mobility	Configures an interface on an ITR to participate in LISP mobility (dynamic-EID roaming).
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 <i>instance id</i> The instance-id of the LISP instance for which the extranet provider policy applies.				
	<i>ipv4 address prefix</i> Defines the IPv4 EID prefixes to be leaked, specified in a.b.c.d/nn form.				
	<i>ipv6 address prefix</i> Defines the IPv6 EID prefixes to be leaked, prefix specified in 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	<table border="1"> <thead> <tr> <th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.2</td><td>This command was introduced.</td></tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.2	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.2	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 <i>instance id</i> The instance-id of the LISP instance for which the extranet provider policy applies.
	<i>ipv4 address prefix</i> Defines the IPv4 EID prefixes to be leaked, specified in a.b.c.d/nn form.
	<i>ipv6 address prefix</i> Defines the IPv6 EID prefixes to be leaked, prefix specified in X:X:X::X:<0-128> form.

eid-table

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 Everest 16.6.2	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 Selects the named VRF table for association with the configured instance. <i>vrf-name</i>

Command Default	Default VRF is associated with instance-id 0.
------------------------	---

Command Modes	router-lisp-instance-service
----------------------	------------------------------

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.2	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	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; padding: 2px;">Release</th><th style="text-align: left; padding: 2px;">Modification</th></tr> </thead> <tbody> <tr> <td style="padding: 2px;">Cisco IOS XE Everest 16.6.2</td><td style="padding: 2px;">This command was introduced.</td></tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.2	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.2	This command was introduced.				

Usage Guidelines

Use the **encapsulation vxlan** command in the service ethernet mode to encapsulate 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)#encapsulation 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 Everest 16.6.2 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 password 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 of 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 Everest 16.6.2 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.

The keyword **proxy-reply** is mandatory in the context of SD-Access for roaming purposes.

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	<i>name-extranet</i> Specifies the name of the extranet created.
---------------------------	--

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

Command Modes	LISP (router-lisp)
----------------------	--------------------

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.2	This command was introduced.

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

instance-id

To create 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 Everest 16.6.2	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 LISPO.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)

ip pim rp-address

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 LISPO
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	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 16.8.1s</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 16.8.1s	This command was introduced.
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

ip pim ssm**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 Specifies the standard IP access list number or name defining the SSM range. access-list
	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 Everest 16.6.2	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 the ITR 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.

locator default-set

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 Everest 16.6.2	This command was introduced.
	Cisco IOS XE Fuji 16.9.1	Introduced prefix-list as part of the command.

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 Everest 16.6.2	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 Everest 16.6.2 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.

map-cache extranet

Command Modes	LISP Instance Service (router-lisp-instance-service)	
Command History	Release	Modification
	Cisco IOS XE Everest 16.6.2 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 Everest 16.6.2 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 <i>prefix-list-name</i> 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	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Fuji 16.9.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Fuji 16.9.1	This command was introduced.
Release	Modification				
Cisco IOS XE Fuji 16.9.1	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.

service

rip	Routing Information Protocol
static	Defines static routes.
locator-set <i>locator-set-name</i>	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 Fuji 16.9.1	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 Everest 16.6.2	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 configure 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 Everest 16.6.1	This command was introduced.
	Cisco IOS XE Fuji 16.9.1	Support for display of proxy database size.

Usage Guidelines	Use the command show lisp instance-id <i>id</i> 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
```

```
show lisp instance-id ipv6 database
```

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
ETR Map-Server(s):	100.110.110.110 prefix-list site2 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/limit	0/65535
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 Everest 16.6.1	This command was introduced.						
	Cisco IOS XE Fuji 16.9.1	Support for display of proxy database size.						
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:								
<pre>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#</pre>								
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 <i>instance-id</i> ipv4 map-cache [<i>destination-EID</i> <i>destination-EID-prefix</i> detail]								
Syntax Description								
<table border="0"> <tr> <td><i>destination-EID</i></td> <td>(Optional) Specifies the IPv4 destination end point identifier (EID) for which the EID-to-RLOC mapping is displayed.</td> </tr> <tr> <td><i>destination-EID-prefix</i></td> <td>(Optional) Specifies the IPv4 destination EID prefix (in the form of <i>a.b.c.d/mn</i>) for which to display the mapping.</td> </tr> <tr> <td>detail</td> <td>(Optional) Displays detailed EID-to-RLOC cache mapping information.</td> </tr> </table>			<i>destination-EID</i>	(Optional) Specifies the IPv4 destination end point identifier (EID) for which the EID-to-RLOC mapping is displayed.	<i>destination-EID-prefix</i>	(Optional) Specifies the IPv4 destination EID prefix (in the form of <i>a.b.c.d/mn</i>) for which to display the mapping.	detail	(Optional) Displays detailed EID-to-RLOC cache mapping information.
<i>destination-EID</i>	(Optional) Specifies the IPv4 destination end point identifier (EID) for which the EID-to-RLOC mapping is displayed.							
<i>destination-EID-prefix</i>	(Optional) Specifies the IPv4 destination EID prefix (in the form of <i>a.b.c.d/mn</i>) 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 Everest 16.6.1	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.								

show lisp instance-id ipv4 map-cache

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

```

show lisp instance-id ipv4 map-cache

```

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

```

```
show lisp instance-id ipv6 map-cache
```

```

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	<i>destination-EID</i> (Optional) Specifies the IPv4 destination end point identifier (EID) for which the EID-to-RLOC mapping is displayed. <i>destination-EID-prefix</i> (Optional) Specifies the IPv4 destination EID prefix (in the form of <i>a.b.c.d/n</i>) 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	<table border="1"> <thead> <tr> <th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td><td>Introduced this command.</td></tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	Introduced this command.
Release	Modification				
Cisco IOS XE Everest 16.6.1	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.

show lisp instance-id ipv4 server

```
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

Cisco IOS XE Everest 16.6.1 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 for UDP registration.

The following are sample outputs of the command :

```
device# show lisp instance-id 100 ipv4 server
LISP Site Registration Information
* = Some locator 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

```

show lisp instance-id ipv6 server

```
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 Everest 16.6.1 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 Everest 16.6.1	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					
<table border="1"> <thead> <tr> <th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td><td>This command was introduced.</td></tr> </tbody> </table>		Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	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	<i>name-prefix-list</i> (Optional) Specifies the prefix-list whose information is displayed.
Command Default	None.
Command Modes	Privileged Exec

show lisp session

Command History	Release	Modification
	Cisco IOS XE Fuji 16.9.1	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 information 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 Everest 16.6.1	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	<table border="1"> <tr> <td><i>locator-address</i></td><td>The name of locator-set that is set as default.</td></tr> <tr> <td>priority <i>priority</i></td><td>(Optional) Specifies the priority (value between 0 and 255) assigned to this PETR. A lower value indicates a higher priority.</td></tr> <tr> <td>weight <i>weight</i></td><td>(Optional) Specifies the percentage of traffic to be load-shared (value between 0 and 100).</td></tr> </table>	<i>locator-address</i>	The name of locator-set that is set as default.	priority <i>priority</i>	(Optional) Specifies the priority (value between 0 and 255) assigned to this PETR. A lower value indicates a higher priority.	weight <i>weight</i>	(Optional) Specifies the percentage of traffic to be load-shared (value between 0 and 100).
<i>locator-address</i>	The name of locator-set that is set as default.						
priority <i>priority</i>	(Optional) Specifies the priority (value between 0 and 255) assigned to this PETR. A lower value indicates a higher priority.						
weight <i>weight</i>	(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 Everest 16.6.2	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.

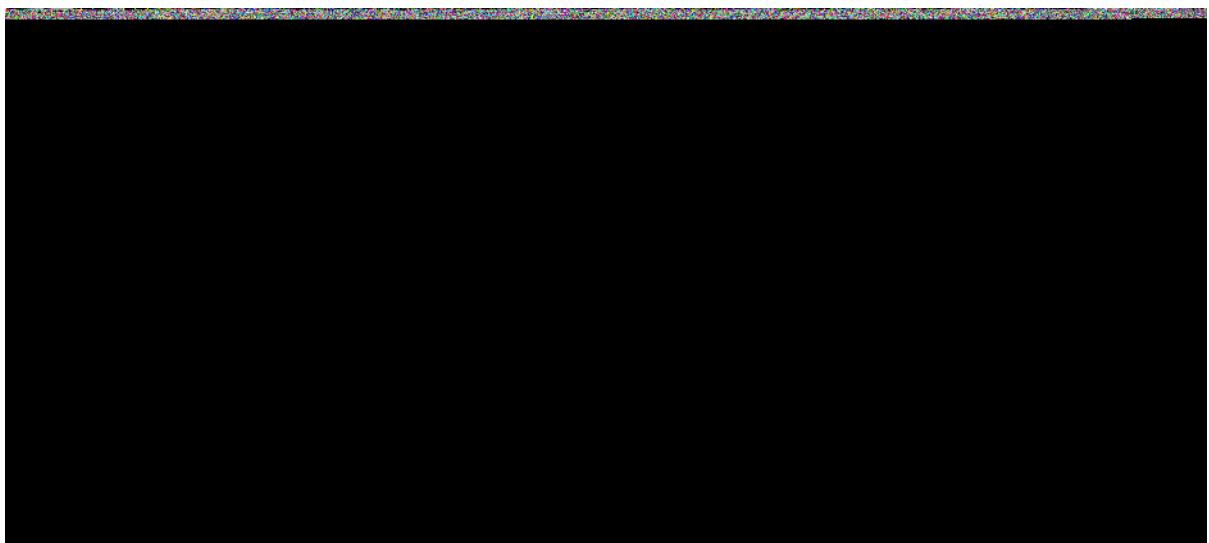
Examples

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**

High Availability

- [High Availability Commands, on page 51](#)
- [Graceful Insertion and Removal, on page 65](#)
- [Cisco StackWise Virtual Commands, on page 69](#)

CHAPTER 9

High Availability Commands

- [main-cpu](#), on page 51
- [mode sso](#), on page 52
- [policy config-sync prc reload](#), on page 52
- [redundancy](#), on page 53
- [redundancy reload peer](#), on page 54
- [redundancy reload shelf](#), on page 55
- [reload](#), on page 55
- [show redundancy](#), on page 57
- [show redundancy config-sync](#), on page 60
- [standby console enable](#), on page 62

main-cpu

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

main-cpu

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Redundancy configuration (config-red)

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.2	This command was implemented on Cisco Catalyst 9400 Series Switches.

Usage Guidelines From the redundancy main configuration submode, use the **standby console enable** command to enable the standby switch.

This example shows how to enter the redundancy main configuration submode and enable the standby switch:

```
Device(config)# redundancy
Device(config-red)# main-cpu
```

mode sso

```
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 Everest 16.6.2	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 supervisor modules to support SSO mode. Redundancy may not work due to differences between the Cisco IOS releases.
- If you perform an online insertion and removal (OIR) of the module, the switch resets during the stateful switchover and the port states are restarted only if the module is in a transient state (any state other than Ready).
- The forwarding information base (FIB) tables are cleared on a switchover. Routed traffic is interrupted until route tables reconverge.

This example shows how to set the redundancy mode to SSO:

```
Device(config) # redundancy
Device(config-red) # mode sso
Device(config-red) #
```

policy config-sync prc reload

To reload the standby switch if a parser return code (PRC) failure occurs during configuration synchronization, use the **policy config-sync reload** command in redundancy configuration mode. To specify that the standby switch is not reloaded if a parser return code (PRC) failure occurs, use the **no** form of this command.

```
policy config-sync {bulk | lbl} prc reload
no policy config-sync {bulk | lbl} prc reload
```

Syntax Description	bulk Specifies bulk configuration mode.				
	lbl Specifies line-by-line (lbl) configuration mode.				
Command Default	The command is enabled by default.				
Command Modes	Redundancy configuration (config-red)				
Command History	<table border="1"> <thead> <tr> <th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.2</td><td>This command was implemented on Cisco Catalyst 9400 Series Switches.</td></tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.2	This command was implemented on Cisco Catalyst 9400 Series Switches.
Release	Modification				
Cisco IOS XE Everest 16.6.2	This command was implemented on Cisco Catalyst 9400 Series Switches.				

This example shows how to specify that the standby switch is not reloaded if a parser return code (PRC) failure occurs during configuration synchronization:

```
Device(config-red)# no policy config-sync bulk prc reload
```

redundancy

To enter redundancy configuration mode, use the **redundancy** command in global configuration mode.

redundancy

Syntax Description	This command has no arguments or keywords.				
Command Default	None				
Command Modes	Global configuration (config)				
Command History	<table border="1"> <thead> <tr> <th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td><td>This command was implemented on Cisco Catalyst 9400 Series Switches.</td></tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was implemented on Cisco Catalyst 9400 Series Switches.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was implemented on Cisco Catalyst 9400 Series Switches.				

Usage Guidelines The redundancy configuration mode is used to enter the main CPU submode, which is used to enable the standby switch.

To enter the main CPU submode, use the **main-cpu** command while in redundancy configuration mode. From the main CPU submode, use the **standby console enable** command to enable the standby switch. Use the **exit** command to exit redundancy configuration mode.

This example shows how to enter redundancy configuration mode:

```
Device(config)# redundancy
Device(config-red) #
```

This example shows how to enter the main CPU submode:

```
Device(config)# redundancy
Device(config-red)# main-cpu
Device(config-r-mc) #
```

redundancy reload peer

Related Commands	Command	Description
	show redundancy	Displays redundancy facility information.

redundancy reload peer

To reload a standby Route Processor (RP) module, use the **redundancy reload peer** command in privileged EXEC mode.

redundancy reload peer

Syntax Description This command has no arguments or keywords.

Command Default No default behavior or values.

Command Modes Privileged EXEC (#)

Command History

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines The **redundancy reload peer** command is used to reset standby RP module when there are any failures, tracebacks, or functionality and behavior mismatches on either one or both active and standby RP modules.

This command does not have an impact on active device operations, assuming a switchover is not required while the standby module is resetting.

Examples

The following example shows how to manually reload the standby RP module:

```
Device# redundancy reload peer
Reload peer? [confirm] y
Preparing to reload peer
```



Note Pressing **enter** or **y** begins the reload. Pressing any other key aborts the reload and returns control to the active RP module.

The following is sample output when a standby RP module is not installed on a router:

```
Device# redundancy reload peer
System is running in SIMPLEX mode, reload anyway? [confirm] n
Peer reload not performed.
```

Command	Description
redundancy	Enters redundancy configuration mode so that the synchronization parameters can be configured.
redundancy reload shelf	Reloads both redundant CPU switch modules.

Command	Description
show redundancy	Displays redundancy facility information.

redundancy reload shelf

To reload both redundant CPU switch modules, use the **redundancy reload shelf** command in privileged EXEC mode.

redundancy reload shelf

Syntax Description This command has no arguments or keywords.

Command Default No default behavior or values.

Command Modes Privileged EXEC (#)

Command History

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines This command causes both CPU switch modules to reload.

Examples The following example shows how to reload the entire shelf:

```
Device# redundancy reload shelf
Reload the entire shelf [confirm] y
Preparing to reload shelf
```

Related Commands

Command	Description
redundancy	Enters redundancy configuration mode so that the synchronization parameters can be configured.
redundancy reload peer	Resets standby RP module when there are any failures, tracebacks, or functionality and behavior mismatches on either one or both active and standby RP modules.
show redundancy	Displays redundancy facility information.

reload

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

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

Syntax Description

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

Command Default

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

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines

If there is more than one switch in the switch stack, and you enter the **reload slot stack-member-number** command, you are not prompted to save the configuration.

Examples

This example shows how to reload the switch stack:

```
Device# reload
System configuration has been modified. Save? [yes/no]: yes
Reload command is being issued on Active unit, this will reload the whole stack
Proceed with reload? [confirm] yes
```

This example shows how to reload a specific stack member:

```
Device# reload slot 6
Proceed with reload? [confirm] y
```

This example shows how to reload a single-switch switch stack (there is only one member switch):

```
Device# reload slot 3
System configuration has been modified. Save? [yes/no]: y
Proceed to reload the whole Stack? [confirm] y
```

show redundancy

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

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

Syntax Description	clients (Optional) Displays information about the redundancy facility client. config-sync (Optional) Displays a configuration synchronization failure or the ignored mismatched command list (MCL). counters (Optional) Displays information about the redundancy facility counter. history (Optional) Displays a log of past status and related information for the redundancy facility. history reload (Optional) Displays a log of past reload information for the redundancy facility. history reverse (Optional) Displays a reverse log of past status and related information for the redundancy facility. slaves (Optional) Displays all slaves in the redundancy facility. <i>slave-name</i> (Optional) The name of the redundancy facility slave to display specific information for. Enter additional keywords to display all clients or counters in the specified slave. clients Displays all redundancy facility clients in the specified slave. counters Displays all counters in the specified slave. states (Optional) Displays information about the redundancy facility state, such as disabled, initialization, standby or active. switchover history (Optional) Displays information about the redundancy facility switchover history. domain default (Optional) Displays the default domain as the domain to display switchover history for.				
Command Default	None				
Command Modes	Privileged EXEC (#)				
Command History	<table border="1"> <thead> <tr> <th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td><td>This command was implemented on Cisco Catalyst 9400 Series Switches.</td></tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was implemented on Cisco Catalyst 9400 Series Switches.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was implemented on Cisco Catalyst 9400 Series Switches.				

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

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

show redundancy

```
-----
Available system uptime = 6 days, 5 hours, 28 minutes
Switchovers system experienced = 0
    Standby failures = 0
    Last switchover reason = none

        Hardware Mode = Duplex
Configured Redundancy Mode = sso
    Operating Redundancy Mode = sso
        Maintenance Mode = Disabled
            Communications = Up

Current Processor Information :
-----
        Active Location = slot 5
        Current Software state = ACTIVE
        Uptime in current state = 6 days, 5 hours, 28 minutes
        Image Version = Cisco IOS Software, Catalyst L3 Switch Software
(CAT9K_IOSXE), Experimental Version 16.x.x [S2C-build-v16x_throttle-4064-/
nobackup/mcpre/BLD-BLD_V16x_THROTTLE_LATEST 102]
Copyright (c) 1986-201x by Cisco Systems, Inc.
Compiled Mon 07-Oct-xx 03:57 by mcpre
        BOOT = bootflash:packages.conf;
        Configuration register = 0x102

Peer Processor Information :
-----
        Standby Location = slot 6
        Current Software state = STANDBY HOT
        Uptime in current state = 6 days, 5 hours, 25 minutes
        Image Version = Cisco IOS Software, Catalyst L3 Switch Software
(CAT9K_IOSXE), Experimental Version 16.x.x [S2C-build-v16x_throttle-4064-/
nobackup/mcpre/BLD-BLD_V16x_THROTTLE_LATEST_20191007_000645 102]
Copyright (c) 1986-201x by Cisco Systems, Inc.
Compiled Mon 07-Oct-xx 03:57 by mcpre
        BOOT = bootflash:packages.conf;
        CONFIG_FILE =
        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
```

show redundancy config-sync

```

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 slaves:

```

Device# show redundancy slaves

Group ID = 1
Slave/Process ID = 6107 Slave Name = [installer]
Slave/Process ID = 6109 Slave Name = [eicored]
Slave/Process ID = 6128 Slave Name = [snmp_subagent]
Slave/Process ID = 8897 Slave Name = [wcm]
Slave/Process ID = 8898 Slave Name = [table_mgr]
Slave/Process ID = 8901 Slave Name = [iosd]

```

```
Device#
```

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

```

Device# show redundancy states

my state = 13 -ACTIVE
peer state = 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 switch to reboot.

mcl Displays commands that exist in the switch's running configuration but are not supported by the image on the standby switch, and forces the standby switch to reboot.

prc Displays a PRC failed command list and forces the standby switch to reboot.

ignored failures mcl Displays the ignored MCL failures.

Command Default None

Command Modes User EXEC
Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Everest 16.6.2	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 switch, the standby switch might not recognize those commands, which causes a configuration mismatch condition. If the syntax check for the command fails on the standby switch during a bulk synchronization, the command is moved into the MCL and the standby switch is reset. To display all the mismatched commands, use the **show redundancy config-sync failures mcl** command.

To clean the MCL, follow these steps:

1. Remove all mismatched commands from the active switch's running configuration.
2. Revalidate the MCL with a modified running configuration by using the **redundancy config-sync validate mismatched-commands** command.
3. Reload the standby switch.

Alternatively, you could ignore the MCL by following these steps:

1. Enter the **redundancy config-sync ignore mismatched-commands** command.
2. Reload the standby switch; the system transitions to SSO mode.



Note If you ignore the mismatched commands, the out-of-synchronization configuration on the active switch and the standby switch still exists.

3. You can verify the ignored MCL with the **show redundancy config-sync ignored mcl** command.

Each command sets a return code in the action function that implements the command. This return code indicates whether or not the command successfully executes. The active switch maintains the PRC after executing a command. The standby switch executes the command and sends the PRC back to the active switch. A PRC failure occurs if these two PRCs do not match. If a PRC error occurs at the standby switch either during bulk synchronization or line-by-line (LBL) synchronization, the standby switch is reset. To display all PRC failures, use the **show redundancy config-sync failures prc** command.

standby console enable

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
```

standby console enable

To enable access to the standby console switch, use the **standby console enable** command in redundancy main configuration submode. To disable access to the standby console switch, use the **no** form of this command.

standby console enable
no standby console enable

Syntax Description This command has no arguments or keywords.

Command Default Access to the standby console switch is disabled.

Command Modes Redundancy main configuration submode

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines This command is used to collect and review specific data about the standby console. The command is useful primarily for Cisco technical support representatives troubleshooting the switch.

This example shows how to enter the redundancy main configuration submode and enable access to the standby console switch:

```
Device(config)# redundancy
Device(config-red)# main-cpu
```

```
Device(config-r-mc)# standby console enable
Device(config-r-mc)#

```

■ standby console enable

CHAPTER 4

Graceful Insertion and Removal

- maintenance-template, on page 65
- router routing protocol shutdown l2, on page 66
- start maintenance, on page 66
- stop maintenance, on page 67
- system mode maintenance, on page 67

maintenance-template

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

maintenance-template *template_name*
no maintenance-template *template_name*

Syntax Description	maintenance-template	Creates a template for GIR with a specific name.
	<i>template_name</i>	Name of the maintenance template.
Command Default	Disabled.	
Command Modes	Global configuration (config)	
Command History	Release	Modification
	Cisco IOS XE Fuji 16.8.1a	This command was introduced.

Example:

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

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

router routing protocol shutdown l2

router routing protocol shutdown l2

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

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

Syntax Description	router Configures instance associated with routing protocol. routing_protocol Routing protocol defined for the template. instance_id Instance ID associated with the routing protocol. shutdown l2 Configures instance to shut down layer 2 interfaces.				
Command Default	Disabled.				
Command Modes	Maintenance template configuration (config-maintenance-temp)				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Fuji 16.8.1a</td><td>This command was introduced.</td></tr> </tbody> </table>	Release	Modification	Cisco IOS XE Fuji 16.8.1a	This command was introduced.
Release	Modification				
Cisco IOS XE Fuji 16.8.1a	This command was introduced.				

Example:

The following example shows how to create an instance for ISIS with an instance ID of one under maintenance template templ1:

```
Device(config)# maintenance template g1
Device(config-maintenance-templ1)# router isis 1
```

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

```
Device(config)# maintenance template g1
Device(config-maintenance-templ1)# shutdown l2
```

start maintenance

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

start maintenance

Syntax Description	start maintenance	Puts the system into maintenance mode.
---------------------------	--------------------------	--

Command Default	Disabled.
Command Modes	Privileged EXEC
Command History	
Release	Modification

Cisco IOS XE Fuji
16.8.1a This command was introduced.

Example:

The following example shows how to start maintenance mode:

```
Device# start maintenance
```

stop maintenance

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

stop maintenance

Command Default	Disabled.
Command Modes	Privileged EXEC
Command History	
Release	Modification

Cisco IOS XE Fuji
16.8.1a This command was introduced.

Example:

The following example shows how to stop maintenance mode:

```
Device# stop maintenance
```

system mode maintenance

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

system mode maintenance

Syntax Description	system mode maintenance	Enters the maintenance configuration mode.
---------------------------	--------------------------------	--

system mode maintenance

Command Default	Disabled.				
Command Modes	Global configuration (config)				
Command History	<table border="1"><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>Cisco IOS XE Fuji 16.8.1a</td><td>This command was introduced.</td></tr></tbody></table>	Release	Modification	Cisco IOS XE Fuji 16.8.1a	This command was introduced.
Release	Modification				
Cisco IOS XE Fuji 16.8.1a	This command was introduced.				

Example:

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

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

CHAPTER 3

Cisco StackWise Virtual Commands

- [clear diagnostic event-log](#), on page 69
- [stackwise-virtual](#), on page 70
- [diagnostic monitor](#), on page 71
- [diagnostic schedule module](#), on page 72
- [diagnostic start](#), on page 75
- [diagnostic stop](#), on page 77
- [domain id](#), on page 78
- [dual-active detection pagp](#), on page 79
- [hw-module beacon switch](#), on page 79
- [hw-module switch slot](#), on page 80
- [hw-module switch usbflash](#), on page 82
- [stackwise-virtual link](#), on page 82
- [stackwise-virtual dual-active-detection](#), on page 83
- [show hw-module switch subslot](#), on page 83
- [show logging onboard switch](#), on page 85
- [show stackwise-virtual](#), on page 88

clear diagnostic event-log

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

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

Syntax Description	
event-type error	Clears the error events.
event-type info	Clears the informative events.
event-type warning	Clears the warning events.
switch num	Clears the events for a specific switch.
module num	Clears the events for a specific module.

switch all	Clears all the event logs from all the switches.
-------------------	--

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

Command History	Release	Modification
	Cisco IOS XE Fuji 16.9.1	This comamnd was introduced

Examples	This example shows how to clear error event logs:
-----------------	---

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

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

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

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

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

Related Commands	Command	Description
	show diagnostic events	Displays the diagnostic event log.

stackwise-virtual

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

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

Syntax Description	stackwise-virtual	Enables Cisco StackWise Virtual.
---------------------------	--------------------------	----------------------------------

Command Default	Disabled.
------------------------	-----------

Command Modes	Global configuration (config)
----------------------	-------------------------------

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

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

Example

The following example shows how to enable Cisco StackWise Virtual :

```
Device(config)# stackwise-virtual
```

diagnostic monitor

To configure health-monitoring diagnostic testing, use the **diagnostic monitor** command in global configuration mode. Use the **no** form of this command to disable testing and to return to the default settings.

diagnostic monitor interval switch number module number test {name | test-id | test-id-range | all} hh:mm:ss milliseconds day [cardindex number]

diagnostic monitor switch number module number test {name | test-id | test-id-range | all} [cardindex number]

diagnostic monitor threshold switch number module number test {name | test-id | test-id-range | all} failure count count [[days number | hours number | milliseconds number | minutes number | runs number | seconds number] cardindex number]

no diagnostic monitor interval switch number module number test {name | test-id | test-id-range | all} [cardindex number]

no diagnostic monitor switch number module number test {name | test-id | test-id-range | all} [cardindex number]

no diagnostic monitor threshold switch number module number test {name | test-id | test-id-range | all} { failure count [[days number | hours number | milliseconds number | minutes number | runs number | seconds number] | cardindex number] | cardindex number} }

Syntax Description	interval	Configures the interval between tests.
	switch number	Specifies the switch number, which is the stack member number. If the switch is a standalone switch, the switch number is 1. If the switch is in a stack, the range is from 1 to 9, depending on the switch member numbers in the stack.
		This keyword is supported only on stacking-capable switches.
	test	Specifies the tests to be run.
	name	Name of the test.
	test-id	ID number of the test.
	test-id-range	Range of test ID numbers. Enter the range as integers separated by a comma and a hyphen (for example, 1,3-6 specifies test IDs 1, 3, 4, 5, and 6).
	all	Specifies all the diagnostic tests.

diagnostic schedule module

<i>hh:mm:ss</i>	Monitoring interval, in hours, minutes, and seconds. Enter the hours from 0 to 24, minutes from 0 to 60, and seconds from 0 to 60.
<i>milliseconds</i>	Monitoring interval, in milliseconds (ms). Enter the test time, in milliseconds, from 0 to 999.
<i>day</i>	Monitoring interval, in days. Enter the number of days between test, from 0 to 20.
threshold	Configures the failure threshold.
failure count <i>count</i>	Sets the failure threshold count.
cardindex <i>number</i>	(Optional) Specifies the card index number.

Command Default Monitoring is disabled, and a failure threshold value is not set.

Command Modes Global configuration (config)

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

Cisco IOS XE Gibraltar 16.11.1 This command was introduced.

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

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

Examples

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

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

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

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

Related Commands

Command	Description
show diagnostic content switch module	Displays online diagnostic test results.

diagnostic schedule module

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

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

Syntax Description

switch <i>switch_num</i>	Specifies the switch number.
module <i>module_num</i>	Specifies the module number.
test	Specifies the diagnostic test suite attribute.
<i>test-id</i>	Identification number for the test to be run. Enter the show diagnostic content command to display the test ID list.
all	Runs all the diagnostic tests.
complete	Selects the complete bootup test suite.
minimal	Selects the minimal bootup test suite.
non-disruptive	Selects the nondisruptive test suite.
per-port	Selects the per-port test suite. per-port is not supported when specifying a scheduled switchover.
port	(Optional) Specifies the port-to-schedule testing.
<i>interface-port-number</i>	(Optional) Port number. The range is from 1-48.
<i>port-number-list</i>	(Optional) Range of port numbers, separated by a hyphen. The range is from 1-48.
all	(Optional) Specifies all the ports.
on month	Specifies the schedule of a test-based diagnostic task. Enter the month name, for example, January or February (either uppercase or lowercase characters).
daily hh:mm	Specifies the daily schedule of a test-based diagnostic task. Enter the time as a two-digit number (for a 24-hour clock) for hours:minutes; the colon (:) is required.

diagnostic schedule module

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

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

Command Modes Global configuration (config)

Command History**Modification**

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

Usage Guidelines Run the **diagnostic schedule switch module test** command to schedule a switchover from the active supervisor engine to the standby supervisor engine.

The **show diagnostic content switch module** command displays the test ID list. The test ID is displayed in the **ScheduleSwitchover** field.

You can specify a periodic switchover (daily or weekly) or a single switchover occurrence at a specific time using these commands:

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



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

Examples

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

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

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

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

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

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

Related Commands	Command	Description
	show diagnostic content	Displays test information, including test ID, test attributes, and supported coverage test levels for all the tests and modules.
	show diagnostic schedule	Displays the current scheduled diagnostic tasks.

diagnostic start

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

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

Syntax Description	switch <i>switch_num</i> module <i>module_num</i> test <i>test-id</i> minimal complete basic per-port non-disruptive all port <i>num</i>	Specifies the switch number. Specifies the module number. Specifies a test to run. Enter the identification number of the test you want to run. Enter the <i>test-id-range</i> or <i>port_range</i> as integers separated by a comma and a hyphen (for example, 1,3-6 specifies test IDs 1, 3, 4, 5, and 6). Runs minimal bootup diagnostic tests. Runs complete bootup diagnostic tests. Runs basic on-demand diagnostic tests. Runs per-port level tests. Runs nondisruptive health-monitoring tests. Runs all the diagnostic tests. (Optional) Specifies the interface port number. The range is from 1-48.
Command Default	None	
Command Modes	Privileged EXEC (#)	
Command History	Release Cisco IOS XE Fuji 16.9.1	Modification This command was introduced.
Usage Guidelines	Run the show diagnostic content command to display the test ID list .	

diagnostic start

Use the **diagnostic stop** command to stop the testing process.

Examples

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

```
Device# diagnostic start switch 1 module 1 test all

Diagnostic[switch 1, module 1]: Running test(s) 2 may disrupt normal system operation and
requires reload
Do you want to continue? [no]: y
Device#
*Jul  5 03:04:49.081 PDT: %DIAG-6-TEST_RUNNING: switch 1, module 1: Running
TestGoldPktLoopback{ID=1} ...
*Jul  5 03:04:49.086 PDT: %DIAG-6-TEST_OK: switch 1, module 1: TestGoldPktLoopback{ID=1}
has completed successfully
*Jul  5 03:04:49.086 PDT: %DIAG-6-TEST_RUNNING: switch 1, module 1: Running
TestPhyLoopback{ID=2} ...
*Jul  5 03:04:49.092 PDT: %DIAG-6-TEST_OK: switch 1, module 1: TestPhyLoopback{ID=2} has
completed successfully
*Jul  5 03:04:49.092 PDT: %DIAG-6-TEST_RUNNING: switch 1, module 1: Running TestThermal{ID=3}
...
*Jul  5 03:04:52.397 PDT: %DIAG-6-TEST_OK: switch 1, module 1: TestThermal{ID=3} has completed
successfully
*Jul  5 03:04:52.397 PDT: %DIAG-6-TEST_RUNNING: switch 1, module 1: Running
TestScratchRegister{ID=4} ...
*Jul  5 03:04:52.414 PDT: %DIAG-6-TEST_OK: switch 1, module 1: TestScratchRegister{ID=4}
has completed successfully
*Jul  5 03:04:52.414 PDT: %DIAG-6-TEST_RUNNING: switch 1, module 1: Running TestPoe{ID=5}
...
*Jul  5 03:04:52.415 PDT: %DIAG-6-TEST_OK: switch 1, module 1: TestPoe{ID=5} has completed
successfully
*Jul  5 03:04:52.415 PDT: %DIAG-6-TEST_RUNNING: switch 1, module 1: Running
TestUnusedPortLoopback{ID=6} ...
*Jul  5 03:04:52.415 PDT: %DIAG-6-TEST_OK: switch 1, module 1: TestUnusedPortLoopback{ID=6}
has completed successfully
*Jul  5 03:04:52.415 PDT: %DIAG-6-TEST_RUNNING: switch 1, module 1: Running
TestPortTxMonitoring{ID=7} ...
*Jul  5 03:04:52.416 PDT: %DIAG-6-TEST_OK: switch 1, module 1: TestPortTxMonitoring{ID=7}
has completed successfully
```

Related Commands

Command	Description
diagnostic bootup level	Configures the diagnostic bootup level.
diagnostic event-log size	Modifies the diagnostic event log size dynamically.
diagnostic monitor	Configures health-monitoring diagnostic testing.
diagnostic ondemand	Configures the on-demand diagnostics.
diagnostic schedule	Sets the diagnostic test schedule for a particular bay, slot, or subslot.
diagnostic stop	Stops a specified diagnostic test.
show diagnostic bootup	Displays the configured diagnostics level at bootup.
show diagnostic content module	Displays the available diagnostic tests.
show diagnostic description	Provides the description for diagnostic tests.

Command	Description
show diagnostic events	Displays the diagnostic event log.
show diagnostic ondemand settings	Displays the settings for the on-demand diagnostics.
show diagnostic result	Displays the diagnostic test results for a module.
show diagnostic schedule	Displays the current scheduled diagnostic tasks.
show diagnostic status	Displays the running diagnostics tests.

diagnostic stop

To stop the testing process, use the **diagnostic stop** command in privileged EXEC mode.

diagnostic stop switch *number* module *module_num*

Syntax Description	switch <i>switch_num</i>	Specifies the switch number.
	module <i>module_num</i>	Specifies the module number.

Command Default None

Command Modes Privileged EXEC (#)

Command History

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

Usage Guidelines Use the **diagnostic start** command to start the testing process.

Examples This example shows how to stop the diagnostic test process:

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

Related Commands	Command	Description
	diagnostic bootup level	Configures the diagnostic bootup level.
	diagnostic event-log size	Modifies the diagnostic event log size dynamically.
	diagnostic monitor	Configures health-monitoring diagnostic testing.
	diagnostic ondemand	Configures the on-demand diagnostics.
	diagnostic schedule	Sets the diagnostic test schedule for a particular bay, slot, or subslot.

Command	Description
diagnostic start	Runs a specified diagnostic test.
show diagnostic bootup	Displays the configured diagnostics level at bootup.
show diagnostic content module	Displays the available diagnostic tests.
show diagnostic description	Provides the description for the diagnostic tests.
show diagnostic events	Displays the diagnostic event log.
show diagnostic ondemand settings	Displays the settings for the on-demand diagnostics.
show diagnostic result	Displays the diagnostic test results for a module.
show diagnostic schedule	Displays the current scheduled diagnostic tasks.
show diagnostic status	Displays the running diagnostics tests.

domain id

To configure Cisco StackWise Virtual domain ID on a switch, use the **domain id** command in the StackWise Virtual configuration mode. To disable, use the **no** form of this command.

domain id
no domain id

Syntax Description	domain	Associates StackWise Virtual configuration with a specific domain.				
	<i>id</i>	Value of the domain ID. The range is from 1 to 255. The default is one.				
Command Default	No domain ID is configured.					
Command Modes	StackWise Virtual configuration (config-stackwise-virtual)					
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Fuji 16.9.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>		Release	Modification	Cisco IOS XE Fuji 16.9.1	This command was introduced.
Release	Modification					
Cisco IOS XE Fuji 16.9.1	This command was introduced.					
Usage Guidelines	This command is optional. You must enable Stackwise Virtual, using the stackwise-virtual command, before configuring the domain ID.					

Example

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

```
Device(config)# stackwise-virtual
Device(config-stackwise-virtual)#domain 2
```

dual-active detection pagp

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

dual-active detection pagp
no dual-active detection pagp

Syntax Description	dual-active detection pagp	Enables pagp dual-active detection.				
Command Default	Enabled.					
Command Modes	StackWise Virtual configuration (config-stackwise-virtual)					
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Fuji 16.9.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Fuji 16.9.1	This command was introduced.	
Release	Modification					
Cisco IOS XE Fuji 16.9.1	This command was introduced.					

Example:

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

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

hw-module beacon switch

To control the blue beacon LED in a field-replaceable unit (FRU), use the **hw-module beacon switch** command in privileged EXEC mode.

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

Syntax Description	<i>switch-number</i>	The switch to access. Valid values are 1 and 2.
	active	Selects the active instance of the switch.
	standby	Selects the standby instance of the switch.
	RP	Selects the route processorfor the selected switch.
	fan-tray	Selects the fan for the selected switch.

hw-module switch slot

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

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

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

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

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

Command Default None

Command Modes Privileged EXEC (#)

Command History**Release**

Cisco IOS XE Fuji
16.9.1 This command was introduced.

Modification

hw-module switch slot

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

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

Syntax Description

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

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

- 1: Linecard slot 1
- 2: Supervisor slot 0
- 3: Supervisor slot 1
- 4: Linecard slot 4

logging onboard Enables logging onboard.

counter (Optional) Configures the logging onboard counter.

environment (Optional) Configures the logging onboard environment.

message (Optional) Configures the logging onboard message.

poe	(Optional) Configures the logging onboard PoE.
temperature	(Optional) Configures the logging onboard temperature.
voltage	(Optional) Configures the logging onboard voltage.
shutdown	Shuts down a field-replaceable unit (FRU).

Command Default None

Command Modes Global configuration (config)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

This example shows how to shut down an FRU:

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

hw-module switch usbflash

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

hw-module switch *switch-number*usbflashunmount

Syntax Description	<i>switch number</i> The switch to access. Valid values are 1 and 2. usbflash unmount Unmounts the USB SSD.				
Command Default	None				
Command Modes	Global Configuration (config)				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Fuji 16.9.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Fuji 16.9.1	This command was introduced.
Release	Modification				
Cisco IOS XE Fuji 16.9.1	This command was introduced.				

Example

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

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

stackwise-virtual link

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

stackwise-virtual link *link-value*
no stackwise-virtual link *link-value*

Syntax Description	stackwise-virtual link	Associates a 10-G or 40-G interface to StackWise Virtual link.
	<i>link value</i>	Domain ID configured for Cisco StackWise Virtual.
Command Default	Disabled.	
Command Modes	Interface configuration (config-if).	

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

Example:

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

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

stackwise-virtual dual-active-detection

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

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

Syntax Description	stackwise-virtual dual-active-detection	Enables Cisco StackWise Virtual dual-active-detection for the specified 10-G or 40-G interface.
---------------------------	--	---

Command Default	Disabled.
------------------------	-----------

Command Modes	Interface configuration (config-if)
----------------------	-------------------------------------

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

Example:

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

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

show hw-module switch subslot

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

```
show hw-module switch subslot
```

show hw-module switch *switch-number* subslot
{slot/subslot | all {attribute | entity | oir | sensors [limits] | subblock | tech-support}}

noshow hw-module switch *switch-number* subslot
{slot/subslot | all {attribute | entity | oir | sensors [limits] | subblock | tech-support}}

Syntax Description

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

Command Default

None

Command Modes

Privileged EXEC (#)

Command History**Release** **Modification**

Cisco IOS XE Fuji 16.9.1	This command was introduced.
--------------------------	------------------------------

Examples

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

```
Device# show hw-module switch 1 subslot all attribute
```

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

```
Device# show hw-module switch 1 subslot all oir
```

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

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

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

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

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

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

show logging onboard switch

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

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

Syntax Description	
switch-number	Switch for which OBFL information is displayed.
active	Displays OBFL information about the active switch.
standby	Displays OBFL information about the standby switch.
RP	Specifies the route processor (RP).
slot	Specifies the slot information.
clilog	Displays the OBFL commands that were entered on the standalone switch or specified stack members.
counter	Displays the counter of the standalone switch or specified stack members.
environment	Displays the unique device identifier (UDI) information for the standalone switch or specified stack members. Also displays the product identification (PID), the version identification (VID), and the serial number for all the connected FRU devices.
message	Displays the hardware-related system messages generated by the standalone switch or specified stack members.
poe	Displays the power consumption of the Power over Ethernet (PoE) ports on the standalone switch or specified stack members.

show logging onboard switch

state	Displays the state of the standalone switch or specified stack members.
status	Displays the status of the standalone switch or specified stack members.
temperature	Displays the temperature of the standalone switch or specified stack members.
uptime	Displays the time at which the standalone switch or specified stack members start, the reason the standalone switch or specified members restart, and the length of time the standalone switch or specified stack members have been running since they last restarted.
voltage	Displays the system voltages of the standalone switch or the specified switch stack members.
continuous	(Optional) Displays the data in the continuous file.
detail	(Optional) Displays both the continuous and summary data.
summary	(Optional) Displays the data in the summary file.
start <i>hh:mm:ss day month year</i>	(Optional) Displays the data from the specified time and date. Enter the time as a 2-digit number for a 24-hour clock. Make sure to use the colons (:), for example, 13:32:45. The range of day is from 1 to 31. The month in upper case or lower case letters. You can enter the full name of the month, such as January or august, or the first three letters of the month, such as jan or Aug. The year is a 4-digit number, such as 2008. The range is from 1970 to 2099.
end <i>hh:mm:ss day month year</i>	(Optional) Displays the data up to the specified time and date. Enter the time as a 2-digit number for a 24-hour clock. Make sure to use the colons (:), for example, 13:32:45. The range of day is from 1 to 31. The month in upper case or lower case letters. You can enter the full name of the month, such as January or august, or the first three letters of the month, such as jan or Aug. The year is a 4-digit number, such as 2008. The range is from 1970 to 2099.

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

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

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

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

Examples

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

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

```
-----
ERROR MESSAGE SUMMARY INFORMATION
-----
MM/DD/YYYY HH:MM:SS Facility-Sev-Name | Count | Persistence Flag
-----
07/06/2018 00:45:23 %IOSXE-2-DIAGNOSTICS_FAILED : >254 LAST Diagnostics Thermal failed
07/06/2018 00:19:57 %IOSXE-2-DIAGNOSTICS_PASSED : >254 LAST Diagnostics Fantray passed
07/07/2018 11:36:10 %IOSXE-2-TRANSCEIVER_INSERTED : >254 LAST Transceiver module inserted
in TenGigabitEthernet1/2/0/5
05/03/2018 05:49:57 %IOSXE-2-TRANSCEIVER_REMOVED : 82 : LAST : Transceiver module removed
from TenGigabitEthernet1/2/0/7
07/07/2018 08:20:36 %IOSXE-2-SPA_REMOVED : >254 LAST SPA removed from subslot 14/0
07/06/2018 01:50:33 %IOSXE-2-SPA_INSERTED : >254 LAST SPA inserted in subslot 11/0
-----
```

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

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

```
-----
OBFL Application Status
-----
Application Uptime:
    Path: /obfl0/
    Cli enable status: enabled
Application Message:
    Path: /obfl0/
    Cli enable status: enabled
Application Voltage:
    Path: /obfl0/
    Cli enable status: enabled
Application Temperature:
    Path: /obfl0/
    Cli enable status: enabled
Application POE:
    Path: /obfl0/
    Cli enable status: enabled
Application Environment:
    Path: /obfl0/
    Cli enable status: enabled
Application Counter:
    Path: /obfl0/
    Cli enable status: enabled
Application Clilog:
    Path: /obfl0/
    Cli enable status: enabled
```

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

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

GREEN

Related Commands

Command	Description
clear logging onboard	Removes the OBFL data from flash memory.

show stackwise-virtual

Command	Description
hw-module logging onboard	Enables OBFL.

show stackwise-virtual

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

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

Syntax Description		
switch number		(Optional) Displays information of a particular switch in the stack.
link		Displays Stackwise Virtual link information.
bandwidth		Displays bandwidth availability for StackWise Virtual.
neighbors		Displays Stackwise Virtual neighbors.
dual-active-detection		Displays Stackwise-Virtual dual-active-detection information.
Command Default	None	
Command Modes	Privileged EXEC (#)	
Command History	Release	Modification
Cisco IOS XE Fuji	16.9.1	This command was introduced.

Example:

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

```
Device# show stackwise-virtual

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

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

```
Device# show stackwise-virtual link

Stackwise Virtual Link (SVL) Information:
-----
Flags:
-----
Link Status
-----
U-Up D-Down
Protocol Status
-----
S-Suspended P-Pending E-Error T-Timeout R-Ready
-----
Switch   SVL      Ports           Link-Status  Protocol-Status
-----  ---      -----           -----       -----
1        1        FortyGigabitEthernet1/1/1    U          R
2        1        FortyGigabitEthernet2/1/1    U          R
```

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

```
Device# show stackwise-virtual bandwidth

Switch  Bandwidth
1          160
2          160
```

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

```
Device#show stackwise-virtual neighbors

Switch Number      Local Interface      Remote Interface
1                  Tengigabitethernet1/0/1  Tengigabitethernet2/0/1
                  Tengigabitethernet1/0/2  Tengigabitethernet2/0/2
2                  Tengigabitethernet2/0/1  Tengigabitethernet1/0/1
                  Tengigabitethernet2/0/2  Tengigabitethernet2/0/2
```

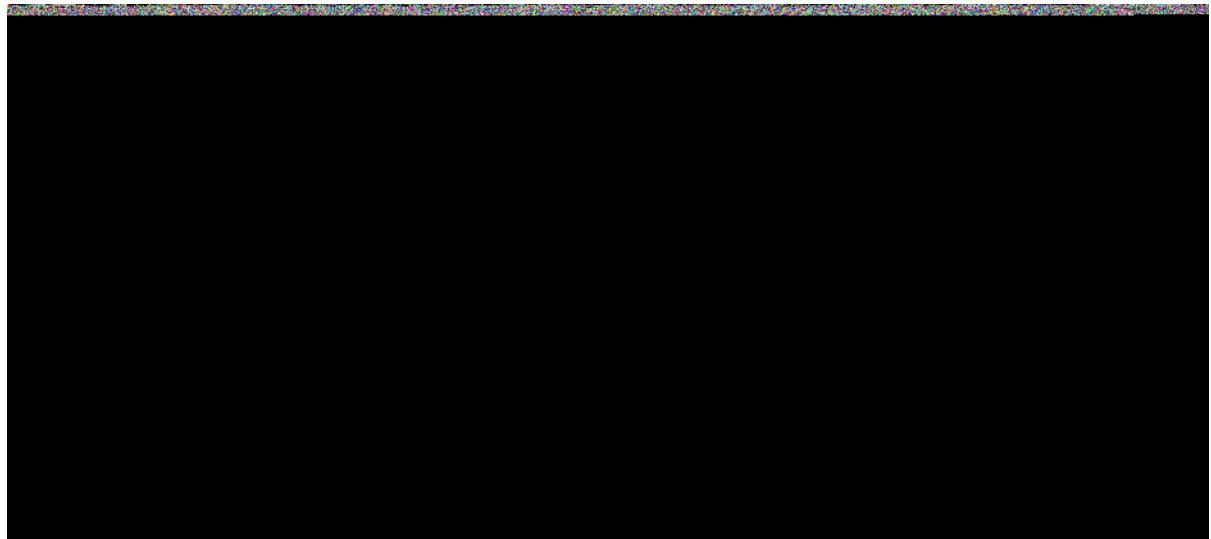
The following is a sample output from the **show stackwise-virtual dual-active-detection** command:

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

Stackwise Virtual Dual-Active-Detection (DAD) Configuration:
Switch Number      Dual-Active-Detection Interface
1                  Tengigabitethernet1/0/10
                  Tengigabitethernet1/0/11
2                  Tengigabitethernet2/0/12
                  Tengigabitethernet2/0/13

Stackwise Virtual Dual-Active-Detection (DAD) Configuration After Reboot:
Switch Number      Dual-Active-Detection Interface
1                  Tengigabitethernet1/0/10
                  Tengigabitethernet1/0/11
2                  Tengigabitethernet2/0/12
                  Tengigabitethernet2/0/13
```

```
show stackwise-virtual
```



PART III

Interface and Hardware Components

- [Interface and Hardware Commands, on page 93](#)

CHAPTER 0

Interface and Hardware Commands

- [debug ilpower](#), on page 94
- [debug interface](#), on page 95
- [debug lldp packets](#), on page 96
- [debug platform poe](#), on page 96
- [duplex](#), on page 97
- [errdisable detect cause](#), on page 98
- [errdisable recovery cause](#), on page 100
- [errdisable recovery interval](#), on page 102
- [hw-module beacon](#), on page 103
- [hw-module subslot mode](#), on page 104
- [interface](#), on page 105
- [interface range](#), on page 107
- [lldp \(interface configuration\)](#), on page 108
- [logging event power-inline-status](#), on page 109
- [mode \(power-stack configuration\)](#), on page 110
- [network-policy](#), on page 111
- [network-policy profile \(global configuration\)](#), on page 112
- [power efficient-ethernet auto](#), on page 113
- [power-priority](#) , on page 114
- [power inline](#), on page 115
- [power inline police](#), on page 117
- [power supply](#), on page 119
- [show beacon all](#), on page 120
- [show eee](#), on page 122
- [show env](#), on page 124
- [show errdisable detect](#), on page 126
- [show errdisable recovery](#), on page 127
- [show hardware led](#), on page 127
- [show hw-module subslot mode](#), on page 130
- [show idprom fan-tray](#), on page 131
- [show ip interface](#), on page 131
- [show interfaces](#), on page 136
- [show interfaces counters](#), on page 139

debug ilpower

- [show interfaces switchport, on page 141](#)
- [show interfaces transceiver, on page 143](#)
- [show inventory, on page 145](#)
- [show logg onboard slot, on page 147](#)
- [show memory platform, on page 148](#)
- [show module, on page 150](#)
- [show mgmt-infra trace messages ilpower, on page 150](#)
- [show mgmt-infra trace messages ilpower-ha, on page 152](#)
- [show mgmt-infra trace messages platform-mgr-poe, on page 152](#)
- [show network-policy profile, on page 153](#)
- [show platform hardware fed active forward, on page 154](#)
- [show platform hardware iomd lc-portmap brief, on page 155](#)
- [show platform hardware iomd portgroups, on page 156](#)
- [show platform resources, on page 157](#)
- [show platform software ilpower, on page 157](#)
- [show platform software process list, on page 159](#)
- [show platform software process slot switch, on page 162](#)
- [show platform software status control-processor, on page 163](#)
- [show processes cpu platform monitor, on page 166](#)
- [show processes memory platform, on page 167](#)
- [show system mtu, on page 170](#)
- [show tech-support , on page 170](#)
- [speed, on page 172](#)
- [switchport block, on page 173](#)
- [system mtu, on page 174](#)
- [voice-signaling vlan \(network-policy configuration\), on page 175](#)
- [voice vlan \(network-policy configuration\), on page 176](#)

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 Cisco IOS XE Everest 16.6.1	Modification 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 stack master. To enable debugging on a stack member, you can start a session from the stack master 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 stack master switch to enable debugging on a member switch without first starting a session.

debug interface

To enable debugging of interface-related activities, use the **debug interface** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

```
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 <i>port-channel-number</i> range is 1 to 48.
	vlan vlan-id Displays debug messages for the specified VLAN. The <i>vlan</i> 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.

debug lldp packets

states	Displays intermediary debug messages when an interface's state transitions.				
Command Default	Debugging is disabled.				
Command Modes	Privileged EXEC				
Command History	<table border="1"> <thead> <tr> <th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td><td>This command was introduced.</td></tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				
Usage Guidelines	<p>If you do not specify a keyword, all debug messages appear.</p> <p>The undebbug interface command is the same as the no debug interface command.</p> <p>When you enable debugging on a switch stack, it is enabled only on the stack master. To enable debugging on a stack member, you can start a session from the stack master 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 stack master switch to enable debugging on a member switch without first starting a session.</p>				

debug lldp packets

To enable debugging of Link Layer Discovery Protocol (LLDP) packets, use the **debug lldp packets** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug lldp packets
no debug lldp packets

Syntax Description	This command has no arguments or keywords.					
Command Default	Debugging is disabled.					
Command Modes	Privileged EXEC					
Command History	<table border="1"> <thead> <tr> <th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td><td>This command was introduced.</td></tr> </tbody> </table>		Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification					
Cisco IOS XE Everest 16.6.1	This command was introduced.					
Usage Guidelines	<p>The undebbug lldp packets command is the same as the no debug lldp packets command.</p> <p>When you enable debugging on a switch stack, it is enabled only on the . To enable debugging on a stack member, you can start a session from the by using the session switch-number EXEC command.</p>					

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	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; padding-bottom: 2px;">Release</th><th style="text-align: right; padding-bottom: 2px;">Modification</th></tr> </thead> <tbody> <tr> <td style="padding-top: 2px;">Cisco IOS XE Everest 16.6.1</td><td style="text-align: right; padding-top: 2px;">This command was introduced.</td></tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				

Usage Guidelines The **undebug platform poe** command is the same as the **no debug platform poe** command.

duplex

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

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

Syntax Description	auto Enables automatic duplex configuration. The port automatically detects whether it should run in full- or half-duplex mode, depending on the attached device mode. full Enables full-duplex mode. half Enables half-duplex mode (only for interfaces operating at 10 or 100 Mbps). You cannot configure half-duplex mode for interfaces operating at 1000 or 10,000 Mbps.				
Command Default	For Gigabit Ethernet ports, the default is auto .				
Command Modes	Interface configuration (config-if)				
Command History	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; padding-bottom: 2px;">Release</th><th style="text-align: right; padding-bottom: 2px;">Modification</th></tr> </thead> <tbody> <tr> <td style="padding-top: 2px;">Cisco IOS XE Everest 16.6.1</td><td style="text-align: right; padding-top: 2px;">This command was introduced.</td></tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	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.				

errdisable detect cause

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



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

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

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

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

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



Caution Changing the interface speed and duplex mode configuration might shut down and reenable the interface during the reconfiguration.

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

Examples

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

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

errdisable detect cause

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

```
errdisable detect cause {all | arp-inspection | bpduguard shutdown vlan | dhcp-rate-limit | dtp-flap | gbic-invalid | inline-power | 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 Everest 16.6.1	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

errdisable recovery cause

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

errdisable recovery interval

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.
Usage Guidelines		A cause (such as all or BPDU guard) is defined as the reason that the error-disabled state occurred. When a cause is detected on an interface, the interface is placed in the error-disabled state, an operational state similar to link-down state.
When a port is error-disabled, it is effectively shut down, and no traffic is sent or received on the port. For the BPDU guard and port-security features, you can configure the switch to shut down only the offending VLAN on the port when a violation occurs, instead of shutting down the entire port.		
If you do not enable the recovery for the cause, the interface stays in the error-disabled state until you enter the shutdown and the no shutdown interface configuration commands. If you enable the recovery for a cause, the interface is brought out of the error-disabled state and allowed to retry the operation again when all the causes have timed out.		
Otherwise, you must enter the shutdown and then the no shutdown commands to manually recover an interface from the error-disabled state.		
You can verify your settings by entering the show errdisable recovery privileged EXEC command.		

Examples

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

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

errdisable recovery interval

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

```
errdisable recovery interval timer-interval
no errdisable recovery interval timer-interval
```

Syntax Description	<i>timer-interval</i> Time to recover from the error-disabled state. The range is 30 to 86400 seconds. The same interval is applied to all causes. The default interval is 300 seconds.	
Command Default	The default recovery interval is 300 seconds.	
Command Modes	Global configuration	
Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.
Usage Guidelines		The error-disabled recovery timer is initialized at a random differential from the configured interval value. The difference between the actual timeout value and the configured value can be up to 15 percent of the configured interval.

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

Examples

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

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

hw-module beacon

To control the beacon LED on a device, use the **hw-module beacon** command in the privileged EXEC mode.

```
hw-module beacon {rp {active | standby} | fan-tray | power-supply ps-slot-number | slotslot-number } { on | off | status}
```

Syntax Description	rp {active standby} Specifies the active or the standby Supervisor to be controlled. fan-tray Specifies the fan tray beacon to be controlled.. power-supply ps-slot-number Specifies the power supply beacon to be controlled. slot slot-num Specifies the slot to be controlled. on Turns the beacon on. off Turns the beacon off. status Displays the status of the beacon.					
Command Default	This command has no default settings.					
Command Modes	Privileged EXEC (#)					
Command History	<table border="1"> <thead> <tr> <th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td>Cisco IOS XE Fuji 16.8.1a</td><td>This command was introduced.</td></tr> </tbody> </table>		Release	Modification	Cisco IOS XE Fuji 16.8.1a	This command was introduced.
Release	Modification					
Cisco IOS XE Fuji 16.8.1a	This command was introduced.					
Usage Guidelines	<p>Use the hw-module beacon command to turn on or off the beacon LEDs. You can monitor the power-supply, fan-tray, line card slots, and supervisor units by turning on the respective beacon LEDs. You can also find the status of these units with the hw-module beacon status command. Turning on the respective beacon LED helps in identifying the unit on the chassis for administrative purposes.</p> <p>Use the hw-module beacon slot slot-number command to enable or disable the module slot LED and also check its status. BLUE indicates the slot LED is on and BLACK indicates that it is off.</p> <p>Use the hw-module beacon rp active {on off} command to enable or disable the active supervisor LED. Similarly the standby supervisor LED can be turned on or off with the hw-module beacon rp standby {on off } command. You can check the status of the supervisor LED using the hw-module beacon rp {active standby} status command. BLUE indicates the supervisor LED is on and BLACK indicates the supervisor LED is off.</p>					

hw-module subslot mode

Use the **hw-module beacon fan-tray {on | off | status}** command to enable or disable the fan tray LED or to check the status of the fan tray LED. BLUE indicates the fan tray LED is on and BLACK indicates that it is off.

Use the **hw-module beacon power-supply ps-slot-number {on | off | status}** command to enable or disable the particular power supply LED, or to check its status. BLUE indicates the power supply LED is on and BLACK indicates the power supply LED is off.

hw-module subslot mode

To control the subscriber line interface (SLI) traffic rate of a device, use the **hw-module subslot mode** command in global configuration mode. To return to the default mode, use the **no** form of this command.

Cisco IOS XE Gibraltar 16.10.x and Earlier Releases

```
hw-module subslot slot/subslot mode [{dynamic | performance}]
no hw-module subslot slot/subslot mode
```

Cisco IOS XE Gibraltar 16.11.1 and Later Releases

```
hw-module subslot slot/subslot mode [{dynamic | performance | static}]
no hw-module subslot slot/subslot mode
```

Syntax Description

slot	Slot number. The range is from 0 to 10.
subslot	Subslot number. The range is from 0 to 0.
dynamic	(Optional) Sets the line card operation modes to dynamic mode.
performance	(Optional) Sets the line card operation modes to performance mode.
static	(Optional) Sets the line card operation modes to static mode.

Command Default

- Until Cisco IOS XE Gibraltar 16.10.x release, the default mode is static.
- Starting in Cisco IOS XE Gibraltar 16.11.1 release, the default mode is dynamic.

Command Modes

Global Configuration (config)

Command History

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines

- **Performance mode:** Allows limited number of front panel interfaces to operate at full 64-byte 10G rate, while keeping the other interfaces in disabled state.

For 7 slot chassis, 8 10G/MGig line card front panel interfaces get activated and provides full 64-byte 10G rate. For 10 slot chassis, 5 front panel interfaces get activated at full 64-byte 10G rate. The other line card interfaces are disabled and do not link up. Disabled front panel interfaces has amber LED on and the **show interfaces** command displays hardware in disabled state.

- **Dynamic mode:** Monitors the system software on how many SLI links are active based on the front panel port link status, and dynamically configures SLI link 64-byte packet max traffic bandwidth.

For 7 slot chassis, when the number of active SLI links exceed 8, system software limits SLI 64-byte packet traffic rate down to 7.5G for all 12 SLIs. For 10 slot chassis, when the number of active SLI links exceed 5, SLI 64-byte packet traffic rate is limited to 6.25G for all 8 SLIs. Otherwise, system software allows full 10G traffic with 64-byte packets on the active SLIs.

- **Static mode:** SLI traffic rate is fixed to 7.5G for both 7 slot chassis and 10 slot chassis.

Examples

The following example shows how to set the line card mode to performance:

```
Device> enable
Device# configure terminal
Device(config)# hw-module subslot 1/0 mode performance
```

Related Commands

Command	Description
show hw-module subslot mode	Displays the line card mode of the platform.
show platform hardware iomd portgroups	Displays the port grouping information of the platform.
show platform hardware iomd lc-portmap brief	Displays the line card port map information of the platform.

interface

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

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

Syntax Description

Auto-Template <i>interface-number</i>	Enables you to configure a auto-template interface. The range is from 1 to 999.
FortyGigabitEthernet <i>switch-number/slot-number/port-number</i>	Enables you to configure a 40-Gigabit Ethernet interface. <ul style="list-style-type: none"> • <i>switch-number</i> — Switch ID. The range is from 1 to 8. • <i>slot-number</i> — Slot number. Value is 1. • <i>port-number</i> — Port number. The range is from 1 to 2.

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

Command Default None

Command Modes Global configuration (config)

	Release	Modification
Command History	Cisco IOS XE Everest 16.6.1	This command was introduced.

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

The following example shows how to configure a tunnel interface:

```
Device# interface Tunnel 15
```

interface range

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

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

Syntax Description		
	Auto-Template <i>interface-number</i>	Enables you to configure a auto-template interface. The range is from 1 to 999.
	FortyGigabitEthernet <i>switch-number/slot-number/port-number</i>	Enables you to configure a 40-Gigabit Ethernet interface. <ul style="list-style-type: none"> • <i>switch-number</i> — Switch ID. The range is from 1 to 8. • <i>slot-number</i> — Slot number. Value is 1. • <i>port-number</i> — Port number. The range is from 1 to 2.
	GigabitEthernet <i>switch-number/slot-number/port-number</i>	Enables you to configure a Gigabit Ethernet IEEE 802.3z interface. <ul style="list-style-type: none"> • <i>switch-number</i> — Switch ID. The range is from 1 to 8. • <i>slot-number</i> — Slot number. The range is from 0 to 1. • <i>port-number</i> — Port number. The range is from 1 to 48.
	Group VI <i>Group VI interface number</i>	Enables you to configure a Group VI interface. The range is from 0 to 9.
	Internal Interface <i>Internal Interface</i>	Enables you to configure an internal interface.
	Loopback <i>interface-number</i>	Enables you to configure a loopback interface. The range is from 0 to 2147483647.
	Null <i>interface-number</i>	Enables you to configure a null interface. The default value is 0.
	Port-channel <i>interface-number</i>	Enables you to configure a port-channel interface. The range is from 1 to 128.

lldp (interface configuration)

TenGigabitEthernet <i>switch-number/slot-number/port-number</i>	<ul style="list-style-type: none"> • <i>switch-number</i> — Switch ID. The range is from 1 to 8. • <i>slot-number</i> — Slot number. The range is from 0 to 1. • <i>port-number</i> — Port number. The range is from 1 to 24 and 37 to 48. <p>Enables you to configure a 10-Gigabit Ethernet interface.</p>				
Tunnel <i>interface-number</i>	Enables you to configure a tunnel interface. The range is from 0 to 2147483647.				
Vlan <i>interface-number</i>	Enables you to configure a switch VLAN. The range is from 1 to 4094.				
Command Default	None				
Command Modes	Global configuration				
Command History	<p>Table 6:</p> <table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				

Examples

This example shows how you can select a set of VLAN interfaces to be configured :

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

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

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	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
```

mode (power-stack configuration)

Syntax Description	This command has no arguments or keywords.	
Command Default	Logging of PoE events is enabled.	
Command Modes	Interface configuration	
Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	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:	
	<pre>Device(config-if)# interface gigabitethernet1/0/1 Device(config-if)# logging event power-inline-status Device(config-if)# </pre>	

mode (power-stack configuration)

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

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

Syntax Description	power-shared	Sets the power stack to operate in power-shared mode. This is the default.
	redundant	Sets the power stack to operate in redundant mode. The largest power supply is removed from the power pool to be used as backup power in case one of the other power supplies fails.
	strict	(Optional) Configures the power stack mode to run a strict power budget. The stack power needs cannot exceed the available power.
Command Default	The default modes are power-shared and nonstrict.	
Command Modes	Power-stack configuration	
Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.
Usage Guidelines	<p>This command is available only on switch stacks running the IP Base or IP Services feature set.</p> <p>To access power-stack configuration mode, enter the stack-power stack power stack name global configuration command.</p> <p>Entering the no mode command sets the switch to the defaults of power-shared and non-strict mode.</p>	

**Note**

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

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

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

In **strict** mode, when a power supply fails and the available power drops below the budgeted power, the system balances the budget through load shedding of powered devices, even if the actual power is less than the available power. In nonstrict mode, the power stack can run in an over-allocated state and is stable as long as the actual power does not exceed the available power. In this mode, a powered device drawing more than normal power could cause the power stack to start shedding loads. This is normally not a problem because most devices do not run at full power. The chances of multiple powered devices in the stack requiring maximum power at the same time is small.

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

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

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

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

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

network-policy

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

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

Syntax Description

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

network-policy profile (global configuration)

Command Default	No network-policy profiles are applied.				
Command Modes	Interface configuration				
Command History	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; padding: 2px;">Release</th> <th style="text-align: right; padding: 2px;">Modification</th> </tr> </thead> <tbody> <tr> <td style="padding: 2px;">Cisco IOS XE Everest 16.6.1</td> <td style="text-align: right; padding: 2px;">This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				

Usage Guidelines	<p>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.</p>
-------------------------	---

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

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

network-policy profile (global configuration)

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

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

Syntax Description	<i>profile-number</i> Network-policy profile number. The range is 1 to 4294967295.				
Command Default	No network-policy profiles are defined.				
Command Modes	Global configuration				
Command History	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; padding: 2px;">Release</th> <th style="text-align: right; padding: 2px;">Modification</th> </tr> </thead> <tbody> <tr> <td style="padding: 2px;">Cisco IOS XE Everest 16.6.1</td> <td style="text-align: right; padding: 2px;">This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				

Usage Guidelines	<p>Use the network-policy profile global configuration command to create a profile and to enter network-policy profile configuration mode.</p> <p>To return to privileged EXEC mode from the network-policy profile configuration mode, enter the exit command.</p> <p>When you are in network-policy profile configuration mode, you can create the profile for voice and voice signaling by specifying the values for VLAN, class of service (CoS), differentiated services code point (DSCP), and tagging mode.</p>
-------------------------	--

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

This example shows how to create network-policy profile 60:

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

power efficient-ethernet auto

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

power efficient-ethernet auto
no power efficient-ethernet auto

Syntax Description This command has no arguments or keywords.

Command Default EEE is disabled.

Command Modes Interface configuration

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

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

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

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

This command does not require a license.

This example shows how to enable EEE for an interface:

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

This example shows how to disable EEE for an interface:

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

power-priority

power-priority

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

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

Syntax Description	<p>high value Sets the power priority for the ports configured as high-priority ports. The range is 1 to 27, with 1 as the highest priority. The high value must be lower than the value set for the low-priority ports and higher than the value set for the switch.</p> <p>low value Sets the power priority for the ports configured as low-priority ports. The range is 1 to 27. The low value must be higher than the value set for the high-priority ports and the value set for the switch.</p> <p>switch value Sets the power priority for the switch. The range is 1 to 27. The switch value must be lower than the values set for the low and high-priority ports.</p>
---------------------------	--

Command Default	If no values are configured, the power stack randomly determines a default priority. The default ranges are 1 to 9 for switches, 10 to 18 for high-priority ports, 19 to 27 for low-priority ports. On non-PoE switches, the high and low values (for port priority) have no effect.
------------------------	--

Command Modes	Switch stack-power configuration
----------------------	----------------------------------

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines	<p>To access switch stack-power configuration mode, enter the stack-power switch switch-number global configuration command.</p> <p>Cisco StackPower power-priority values determine the order for shutting down switches and ports when power is lost and load shedding must occur. Priority values are from 1 to 27; the highest numbers are shut down first.</p> <p>We recommend that you configure different priority values for each switch and for its high priority ports and low priority ports to limit the number of devices shut down at one time during a loss of power. If you try to configure the same priority value on different switches in a power stack, the configuration is allowed, but you receive a warning message.</p>
-------------------------	--



Note This command is available only on switch stacks running the IP Base or IP Services feature set.

Examples	This is an example of setting the power priority for switch 1 in power stack a to 7, for the high-priority ports to 11, and for the low-priority ports to 20.
-----------------	---

```

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

```

power inline

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

```

power inline {auto [max max-wattage] | 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.

power inline

The default port priority is low.

Command Default	Interface configuration	
Command History	Release	Modification

Cisco IOS XE Everest 16.6.1 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	(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.
errdisable	

action log	(Optional) Configures the device to generate a syslog message while still providing power to a connected device if the real-time power consumption exceeds the maximum power allocation on the port.				
Command Default	Policing of the real-time power consumption of the powered device is disabled.				
Command Modes	Interface configuration				
Command History	<table border="1"> <thead> <tr> <th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td><td>This command was introduced.</td></tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				

Usage Guidelines	<p>This command is supported only on the LAN Base image.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>When PoE is enabled, the device senses the real-time power consumption of the powered device. This feature is called <i>power monitoring</i> or <i>power sensing</i>. The device also polices the power usage with the <i>power policing</i> feature.</p> <p>When power policing is enabled, the device uses one of the these values as the cutoff power on the PoE port in this order:</p> <ol style="list-style-type: none"> 1. The user-defined power level that limits the power allowed on the port when you enter the power inline auto max max-wattage or the power inline static max max-wattage interface configuration command 2. The device automatically sets the power usage of the device by using CDP power negotiation or by the IEEE classification and LLDP power negotiation. <p>If you do not manually configure the cutoff-power value, the device automatically determines it by using CDP power negotiation or the device IEEE classification and LLDP power negotiation. If CDP or LLDP are not enabled, the default value of 30 W is applied. However without CDP or LLDP, the device does not allow devices to consume more than 15.4 W of power because values from 15400 to 30000 mW are only allocated based on CDP or LLDP requests. If a powered device consumes more than 15.4 W without CDP or LLDP negotiation, the device might be in violation of the maximum current <i>I_{max}</i> limitation and might experience an <i>I_{cut}</i> 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.</p> <p>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.</p> <p>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</p>
-------------------------	--

(or *cutoff power*) on the port, the device either turns power off to the port, or the device generates a syslog message and updates the LEDs (the port LEDs are blinking amber) while still providing power to the device.

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

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

Caution

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

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

Examples

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

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

power supply

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

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

Syntax Description	<i>stack-member-number</i>	Stack member number for which to configure the internal power supplies. The range is 1 to 9, depending on the number of switches in the stack. This parameter is available only on stacking-capable switches.
	slot	Selects the switch power supply to set.
	A	Selects the power supply in slot A.
	B	Selects the power supply in slot B.
		Note Power supply slot B is the closest slot to the outer edge of the switch.
	off	Sets the switch power supply to off.

show beacon all

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 Everest 16.6.1 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					

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} | fan-tray | power-supply ps-slot-number | slot slot-number} | all}
```

Syntax Description **rp {active | standby}** Specifies the active or the standby Supervisor whose beacon LED status is to be displayed.

slot <i>slot-num</i>	Specifies the slot whose beacon LED status is to be displayed.
fan-tray	Specifies that the status of fan tray beacon is to be displayed.
power-supply <i>ps-slot-number</i>	Specifies the power supply whose beacon LED status is to be displayed.
all	Displays the status of all beacon LEDs.

Command History	Release	Modification
	Cisco IOS XE Fuji 16.9.1	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 on a 7-slot device.

```
Device#show beacon all
Slot#      Beacon Status
-----
1          OFF
2          OFF
3          OFF
*4         OFF
5          OFF
6          OFF
7          OFF
-----
Power-Supply#   Beacon Status
-----
4          OFF
8          OFF
-----
FANTRAY BEACON:  OFF
Switch#
```

Following is a sample output of **show beacon rp** command on a 7-slot device

```
Device#show beacon rp active
Slot#      Beacon Status
-----
3          ON

Switch#show beacon rp standby
Slot#      Beacon Status
-----
4          OFF
```

show eee

The following example displays the status of fantray:

```
Device#show beacon fantray
-----
FANTRAY BEACON: ON
Switch#
```

show eee

To display Energy Efficient Ethernet (EEE) information for an interface, use the **show eee** command in EXEC mode.

Syntax Description	capabilities Displays EEE capabilities for the specified interface. status Displays EEE status information for the specified interface. interface <i>interface-id</i> Specifies the interface for which to display EEE capabilities or status information.				
Command Default	None				
Command Modes	User EXEC Privileged EXEC				
Command History	<table border="1"> <thead> <tr> <th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td><td>This command was introduced.</td></tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				
Usage Guidelines	You can enable EEE on devices that support low power idle (LPI) mode. Such devices can save power by entering LPI mode during periods of low power utilization. In LPI mode, systems on both ends of the link can save power by shutting down certain services. EEE provides the protocol needed to transition into and out of LPI mode in a way that is transparent to upper layer protocols and applications. To check if an interface is EEE capable, use the show eee capabilities command. You can enable EEE on an interface that is EEE capable by using the power efficient-ethernet auto interface configuration command. To view the EEE status, LPI status, and wake error count information for an interface, use the show eee status command.				

This is an example of output from the **show eee capabilities** command on an interface where EEE is enabled:

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

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

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

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

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

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

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

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

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

show env

Table 7: show eee status Field Descriptions

Field	Description
EEE (efficient-ethernet)	<p>The EEE status for the interface. This field can have any of the following values:</p> <ul style="list-style-type: none"> • N/A—The port is not capable of EEE. • Disabled—The port EEE is disabled. • Disagreed—The port EEE is not set because a remote link partner might be incompatible with EEE; either it is not EEE capable, or its EEE setting is incompatible. • Operational—The port EEE is enabled and operating. <p>If the interface speed is configured as 10 Mbps, EEE is disabled internally. When the interface speed moves back to auto, 100 Mbps or 1000 Mbps, EEE becomes active again.</p>
Rx/Tx LPI Status	<p>The Low Power Idle (LPI) status for the link partner. These fields can have any of the following values:</p> <ul style="list-style-type: none"> • N/A—The port is not capable of EEE. • Interrupted—The link partner is in the process of moving to low power mode. • Low Power—The link partner is in low power mode. • None—EEE is disabled or not capable at the link partner side. • Received—The link partner is in low power mode and there is traffic activity. <p>If an interface is configured as half-duplex, the LPI status is None, which means the interface cannot be in low power mode until it is configured as full-duplex.</p>
Wake Error Count	<p>The number of PHY wake-up faults that have occurred. A wake-up fault can occur when EEE is enabled and the connection to the link partner is broken.</p> <p>This information is useful for PHY debugging.</p>

show env

To display fan, temperature, and power information, use the **show env** command in EXEC mode.

show env {all | fan | power [{all | switch [stack-member-number]}] | stack [stack-member-number] | temperature [status]}

Syntax Description	all Displays the fan and temperature environmental status and the status of the internal power supplies.
fan	Displays the switch fan status.
power	Displays the internal power status of the active switch.
all	(Optional) Displays the status of all the internal power supplies in a standalone switch when the command is entered on the switch, or in all the stack members when the command is entered on the active switch.
switch	(Optional) Displays the status of the internal power supplies for each switch in the stack or for the specified switch. This keyword is available only on stacking-capable switches.
<i>stack-member-number</i>	(Optional) Number of the stack member for which to display the status of the internal power supplies or the environmental status.
stack	Displays all environmental status for each switch in the stack or for the specified switch. This keyword is available only on stacking-capable switches.
temperature	Displays the switch temperature status.
status	(Optional) Displays the switch internal temperature (not the external temperature) and the threshold values.

Command Default	None				
Command Modes	User EXEC Privileged EXEC				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				

Usage Guidelines	Use the show env EXEC command to display the information for the switch being accessed—a standalone switch or the active switch. Use this command with the stack and switch keywords to display all information for the stack or for the specified stack member. If you enter the show env temperature status command, the command output shows the switch temperature state and the threshold level. You can also use the show env temperature command to display the switch temperature status. The command output shows the green and yellow states as <i>OK</i> and the red state as <i>FAULTY</i> . If you enter the show env all command, the command output is the same as the show env temperature status command output.
-------------------------	--

show errdisable detect**Examples**

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

Table 8: States in the show env temperature status Command Output

State	Description
Green	The switch temperature is in the <i>normal</i> operating range.
Yellow	The temperature is in the <i>warning</i> range. You should check the external temperature around the switch.
Red	The temperature is in the <i>critical</i> range. The switch might not run properly if the temperature is in this range.

show errdisable detect

To display error-disabled detection status, use the **show errdisable detect** command in EXEC mode.

show errdisable detect

Syntax Description	This command has no arguments or keywords.	
Command Default	None	
Command Modes	User EXEC Privileged EXEC	
Command History		
Release	Modification	
Cisco IOS XE Everest 16.6.1	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.

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 Everest 16.6.1	This command was introduced.
Usage Guidelines	A gbic-invalid error-disable reason refers to an invalid small form-factor pluggable (SFP) module interface.	
 Note	Though visible in the output, the unicast-flood field is not valid.	

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

show hardware led

To display the status of hardware components on the device, use the **show hardware led** command in privileged EXEC mode.

show hardware led [port [FortyGigabitEthernet *interface-number* | TenGigabitEthernet *interface-number* | GigabitEthernet *interface-number* | status]]

Syntax Description	FortyGigabitEthernet <i>interface-number</i>	Specifies the FortyGigabit interface whose LED status is to be displayed
	TenGigabitEthernet <i>interface-number</i>	Specifies the Tengigabit interface whose LED status is to be displayed.
	GigabitEthernet <i>interface-number</i>	Specifies the One Gigabit interface whose LED status is to be displayed.
	status	Displays the status of the ports on the device.

show hardware led

Command History	Release	Modification		
	Cisco IOS XE Fuji 16.8.1a	This command was introduced.		
Command Default	This command has no default settings.			
Command Modes	Privileged EXEC (#)			
Usage Guidelines				
<p>The show hardware led command displays the status of ports on the Line Cards and Supervisors, status of PowerSupply and Fan tray modules, and the status of RJ45 console.</p> <p>On a Supervisor there are four PORT SET ENABLED LEDs, each representing a group of ports. Port numbers 1 to 4 form Group 1 (G1), Port numbers 5 to 8 form Group 2 (G2), Port number 9 is Group 3 (G3) and Port number 10 is Group 4 (G4). Status of each group for an active or standby supervisor is displayed.</p> <p>The command displays the following colors to indicate status of the PORT LEDs:</p> <ul style="list-style-type: none"> • GREEN—Indicates the interface is up. • BLACK—Indicates the interface is down. • AMBER—Indicates the interface ADMIN is down. <p>The command displays the following colors to indicate the status of Line Cards (LC):</p> <ul style="list-style-type: none"> • AMBER—Indicates the LC is booting up. • GREEN—Indicates the LC is up and running. • RED—Indicates the LC has a problem or is disabled. <p>Status of BEACON LED for fantray, power-supply, line cards and supervisor moodules are indicated by the following colours:</p> <ul style="list-style-type: none"> • BLUE—Indicates the Beacon LED is On. • BLACK—Indicates the Beacon LED is Off. <p>Status of SYSTEM LED is indicated by the following colors:</p> <ul style="list-style-type: none"> • GREEN—Indicates all components are up and running. • RED—Indicates that temperature exceeds either the critical temperature or the shutdown threshold; or fantray is either removed or has failed. • ORANGE—Indicates that temperature exceeds the warning threshold; or fantray experiences partial fails; or active power supply failed. 				

For more information on LEDs refer [Cisco Catalyst 9400 Series Switches Hardware Installation Guide](#).

Sample output of **show hardware led** command

```
Device#show hardware led
SWITCH: C9407R
SYSTEM: GREEN
```

Line Card : 1
 PORT STATUS: (24) Te1/0/1:BLACK Te1/0/2:BLACK Te1/0/3:BLACK Te1/0/4:BLACK Te1/0/5:BLACK
 Te1/0/6:BLACK Te1/0/7:BLACK Te1/0/8:BLACK Te1/0/9:BLACK Te1/0/10:BLACK Te1/0/11:BLACK
 Te1/0/12:BLACK Te1/0/13:BLACK Te1/0/14:BLACK Te1/0/15:BLACK Te1/0/16:BLACK Te1/0/17:BLACK
 Te1/0/18:BLACK Te1/0/19:BLACK Te1/0/20:BLACK Te1/0/21:BLACK Te1/0/22:BLACK Te1/0/23:BLACK
 Te1/0/24:BLACK
 BEACON: BLUE

STATUS: GREEN

Line Card : 2
 PORT STATUS: (48) Gi2/0/1:ACT_GREEN Gi2/0/2:ACT_GREEN Gi2/0/3:BLACK Gi2/0/4:BLACK
 Gi2/0/5:BLACK Gi2/0/6:BLACK Gi2/0/7:BLACK Gi2/0/8:BLACK Gi2/0/9:BLACK Gi2/0/10:BLACK
 Gi2/0/11:BLACK Gi2/0/12:BLACK Gi2/0/13:BLACK Gi2/0/14:BLACK Gi2/0/15:BLACK Gi2/0/16:BLACK
 Gi2/0/17:BLACK Gi2/0/18:BLACK Gi2/0/19:BLACK Gi2/0/20:BLACK Gi2/0/21:BLACK Gi2/0/22:BLACK
 Gi2/0/23:ACT_GREEN Gi2/0/24:BLACK Gi2/0/25:ACT_GREEN Gi2/0/26:BLACK Gi2/0/27:BLACK
 Gi2/0/28:BLACK Gi2/0/29:BLACK Gi2/0/30:BLACK Gi2/0/31:BLACK Gi2/0/32:BLACK Gi2/0/33:BLACK
 Gi2/0/34:BLACK Gi2/0/35:BLACK Gi2/0/36:BLACK Gi2/0/37:BLACK Gi2/0/38:BLACK Gi2/0/39:BLACK
 Gi2/0/40:BLACK Gi2/0/41:BLACK Gi2/0/42:BLACK Gi2/0/43:BLACK Gi2/0/44:BLACK Gi2/0/45:ACT_GREEN
 Gi2/0/46:BLACK Gi2/0/47:BLACK Gi2/0/48:BLACK
 BEACON: BLUE

STATUS: GREEN

SUPERVISOR: ACTIVE
 PORT STATUS: (10) Te3/0/1:BLACK Te3/0/2:BLACK Te3/0/3:BLACK Te3/0/4:BLACK Te3/0/5:BLACK
 Te3/0/6:BLACK Te3/0/7:BLACK Te3/0/8:BLACK Fo3/0/9:BLACK Fo3/0/10:BLACK

BEACON: BLUE

GROUP LED: UPLINK-G1:GREEN UPLINK-G2:BLACK UPLINK-G3:BLACK UPLINK-G4:BLACK

SUPERVISOR: STANDBY
 PORT STATUS: (10) Te4/0/1:BLACK Te4/0/2:BLACK Te4/0/3:BLACK Te4/0/4:BLACK Te4/0/5:BLACK
 Te4/0/6:BLACK Te4/0/7:BLACK Te4/0/8:BLACK Fo4/0/9:BLACK Fo4/0/10:BLACK

BEACON: BLUE

GROUP LED: UPLINK-G1:BLACK UPLINK-G2:BLACK UPLINK-G3:GREEN UPLINK-G4:BLACK

Line Card : 5
 PORT STATUS: (48) Gi5/0/1:BLACK Gi5/0/2:BLACK Gi5/0/3:BLACK Gi5/0/4:BLACK Gi5/0/5:BLACK
 Gi5/0/6:BLACK Gi5/0/7:BLACK Gi5/0/8:BLACK Gi5/0/9:BLACK Gi5/0/10:BLACK Gi5/0/11:BLACK
 Gi5/0/12:BLACK Gi5/0/13:BLACK Gi5/0/14:BLACK Gi5/0/15:BLACK Gi5/0/16:BLACK Gi5/0/17:BLACK
 Gi5/0/18:BLACK Gi5/0/19:BLACK Gi5/0/20:BLACK Gi5/0/21:BLACK Gi5/0/22:BLACK Gi5/0/23:ACT_GREEN
 Gi5/0/24:BLACK Gi5/0/25:ACT_GREEN Gi5/0/26:BLACK Gi5/0/27:BLACK Gi5/0/28:BLACK Gi5/0/29:BLACK
 Gi5/0/30:BLACK Gi5/0/31:BLACK Gi5/0/32:BLACK Gi5/0/33:BLACK Gi5/0/34:BLACK Gi5/0/35:BLACK
 Gi5/0/36:BLACK Gi5/0/37:BLACK Gi5/0/38:BLACK Gi5/0/39:BLACK Gi5/0/40:BLACK Gi5/0/41:ACT_GREEN
 Gi5/0/42:BLACK Gi5/0/43:BLACK Gi5/0/44:BLACK Gi5/0/45:ACT_GREEN Gi5/0/46:BLACK Gi5/0/47:BLACK
 Gi5/0/48:ACT_GREEN

BEACON: BLUE

STATUS: GREEN

Line Card : 6
 PORT STATUS: (48) Gi6/0/1:BLACK Gi6/0/2:BLACK Gi6/0/3:BLACK Gi6/0/4:BLACK Gi6/0/5:BLACK
 Gi6/0/6:BLACK Gi6/0/7:BLACK Gi6/0/8:BLACK Gi6/0/9:BLACK Gi6/0/10:BLACK Gi6/0/11:BLACK
 Gi6/0/12:BLACK Gi6/0/13:BLACK Gi6/0/14:BLACK Gi6/0/15:BLACK Gi6/0/16:BLACK Gi6/0/17:BLACK
 Gi6/0/18:BLACK Gi6/0/19:BLACK Gi6/0/20:BLACK Gi6/0/21:BLACK Gi6/0/22:BLACK Gi6/0/23:BLACK

show hw-module subslot mode

```

Gi6/0/24:BLACK Gi6/0/25:BLACK Gi6/0/26:BLACK Gi6/0/27:BLACK Gi6/0/28:BLACK Gi6/0/29:BLACK
Gi6/0/30:BLACK Gi6/0/31:BLACK Gi6/0/32:BLACK Gi6/0/33:BLACK Gi6/0/34:BLACK Gi6/0/35:BLACK
Gi6/0/36:BLACK Gi6/0/37:BLACK Gi6/0/38:BLACK Gi6/0/39:BLACK Gi6/0/40:BLACK Gi6/0/41:ACT_GREEN
Gi6/0/42:BLACK Gi6/0/43:BLACK Gi6/0/44:BLACK Gi6/0/45:BLACK Gi6/0/46:BLACK Gi6/0/47:BLACK
Gi6/0/48:BLACK
BEACON: BLUE
STATUS: GREEN

Line Card : 7
PORT STATUS: (48) Gi7/0/1:BLACK Gi7/0/2:BLACK Gi7/0/3:BLACK Gi7/0/4:BLACK Gi7/0/5:BLACK
Gi7/0/6:BLACK Gi7/0/7:BLACK Gi7/0/8:BLACK Gi7/0/9:BLACK Gi7/0/10:BLACK Gi7/0/11:BLACK
Gi7/0/12:BLACK Gi7/0/13:BLACK Gi7/0/14:BLACK Gi7/0/15:BLACK Gi7/0/16:BLACK Gi7/0/17:BLACK
Gi7/0/18:BLACK Gi7/0/19:BLACK Gi7/0/20:BLACK Gi7/0/21:BLACK Gi7/0/22:BLACK Gi7/0/23:BLACK
Gi7/0/24:BLACK Te7/0/25:BLACK Te7/0/26:BLACK Te7/0/27:BLACK Te7/0/28:BLACK Te7/0/29:BLACK
Te7/0/30:BLACK Te7/0/31:BLACK Te7/0/32:BLACK Te7/0/33:BLACK Te7/0/34:BLACK Te7/0/35:BLACK
Te7/0/36:BLACK Te7/0/37:BLACK Te7/0/38:BLACK Te7/0/39:BLACK Te7/0/40:BLACK Te7/0/41:BLACK
Te7/0/42:BLACK Te7/0/43:BLACK Te7/0/44:BLACK Te7/0/45:BLACK Te7/0/46:BLACK Te7/0/47:BLACK
Te7/0/48:BLACK
BEACON: BLUE
STATUS: GREEN

RJ45 CONSOLE: GREEN
FANTRAY STATUS: GREEN
FANTRAY BEACON: BLUE
POWER-SUPPLY 1 BEACON: BLUE
POWER-SUPPLY 2 BEACON: BLUE

```

show hw-module subslot mode

To display the line card mode of the platform, use the **show hw-module subslot mode** command in privileged EXEC mode.

show hw-module subslot slot/subslot mode

Syntax Description

slot Slot number. The range is from 0 to 10.

subslot Subslot number. The range is from 0 to 0.

Command Modes

Privileged EXEC (#)

Command History
Release

Cisco IOS XE Everest
16.6.1

Modification

This command was introduced.

Examples

The following is sample output from the **show hw-module subslot mode** command:

```

Device# show hw-module subslot 1/0 mode

subslot [1/0] mode: dynamic

```

show idprom fan-tray

To display the serial number for the fan-tray component and the chassis, use the **show idprom fan-tray** command in privileged EXEC mode.

```
show idprom fan-tray
```

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced.
Cisco IOS XE Fuji 16.8.1a	The output of the command was enhanced to include Chassis Serial Number in the command output.

The following is sample output from the **show idprom fan-tray** command:

```
Device#show idprom fan tray
Fan Tray Idprom:

Controller Type      : 3196
Hardware Revision   : 0.1
Top Assy. Revision  : 24
Deviation Number    : 0
PCB Serial Number   : FXS2006018B
Chassis Serial Number: FXS2009Q09Z
RMA Test History    : 00
RMA Number          : 0-0-0-0
RMA History         : 00
CLEI Code           : 0
ECI Number          : 0
Product Identifier (PID) : WS-XFAN7
Version Identifier (VID) : V00
Manufacturing Test Data : 00 00 00 00 00 00 00 00
Field Diagnostics Data : 00 00 00 00 00 00 00 00
Environment Monitor Data : 03 00 00 00 15 E1 5E 00
                                A9
Environment Monitor Data : 00 06 00 FA
```

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	<i>type</i> (Optional) Interface type.
	<i>number</i> (Optional) Interface number.

show ip interface

brief (Optional) Displays a summary of the usability status information for each interface.

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 Everest 16.6.1	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.

show ip interface**Table 9: 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.
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.

Field	Description
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 10: show ip interface brief Field Descriptions

Field	Description
Interface	Type of interface.
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.

show interfaces

Field	Description
Method	The Method field has the following possible values: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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] | debounce | description | etherchannel | flowcontrol | private-vlan mapping | pruning | stats | status [{err-disabled}] | trunk}]
```

Syntax Description		
	<i>interface-id</i>	(Optional) ID of the interface. Valid interfaces include physical ports (including type, stack member for stacking-capable switches, module, and port number) and port channels. The port channel range is 1 to 48.
	vlan <i>vlan-id</i>	(Optional) VLAN identification. The range is 1 to 4094.
	accounting	(Optional) Displays accounting information on the interface, including active protocols and input and output packets and octets. Note The display shows only packets processed in software; hardware-switched packets do not appear.
	capabilities	(Optional) Displays the capabilities of all interfaces or the specified interface, including the features and options that you can configure on the interface. Though visible in the command line help, this option is not available for VLAN IDs.
	module <i>number</i>	(Optional) Displays capabilities of all interfaces on the switch or specified stack member. This option is not available if you entered a specific interface ID.
	description	(Optional) Displays the administrative status and description set for interfaces.
	etherchannel	(Optional) Displays interface EtherChannel information.
	flowcontrol	(Optional) Displays interface flow control information.
	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.
	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	

show interfaces

Command Modes	Privileged EXEC (#)	
Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines The **show interfaces capabilities** command with different keywords has these results:

- Use the **show interface capabilities module number** command to display the capabilities of all interfaces on that switch in the stack. If there is no switch with that module number in the stack, there is no output.
- Use the **show interfaces interface-id capabilities** to display the capabilities of the specified interface.
- Use the **show interfaces capabilities** (with no module number or interface ID) to display the capabilities of all interfaces in the stack.



Note The field **Last Input** displayed in the command output indicates the number of hours, minutes, and seconds since the last packet was successfully received by an interface and processed by the CPU on the device. This information can be used to know when a dead interface failed.

Last Input is not updated by fast-switched traffic.

The field **output** displayed in the command output indicates the number of hours, minutes, and seconds since the last packet was successfully transmitted by the interface. The information provided by this field can be useful for knowing when a dead interface failed.

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

```
Device# show interfaces gigabitethernet1/0/2 description
Interface                  Status      Protocol Description
Gi1/0/2                   up         down     Connects to Marketing
```

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

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

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

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

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

```
Total      1165354    136205310      570800      91731594
```

This is an example of output from the **show interfaces 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 Gi1/0/1	Vlans allowed on trunk			
Port Gi1/0/1	none			
Port Gi1/0/1	Vlans allowed and active in management domain			
Port Gi1/0/1	none			
Port Gi1/0/1	Vlans in spanning tree forwarding state and not pruned			
Port Gi1/0/1	none			

show interfaces counters

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

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

Syntax Description	<i>interface-id</i>	(Optional) ID of the physical interface, including type, stack member (stacking-capable switches only) module, and port number.
	errors	(Optional) Displays error counters.
	etherchannel	(Optional) Displays EtherChannel counters, including octets, broadcast packets, multicast packets, and unicast packets received and sent.
	module	(Optional) Displays counters for the specified stack member.
	<i>stack-member-number</i>	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.

show interfaces counters

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 Everest 16.6.1 This command was introduced.

Usage Guidelines If you do not enter any keywords, all counters for all interfaces are included.

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

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

<output truncated>
```

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

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

<output truncated>
```

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

```
Device# show interfaces counters protocol status
Protocols allocated:
Vlan1: Other, IP
Vlan20: Other, IP, ARP
Vlan30: Other, IP, ARP
Vlan40: Other, IP, ARP
Vlan50: Other, IP, ARP
Vlan60: Other, IP, ARP
Vlan70: Other, IP, ARP
Vlan80: Other, IP, ARP
Vlan90: Other, IP, ARP
```

```
Vlan900: Other, IP, ARP
Vlan3000: Other, IP
Vlan3500: Other, IP
GigabitEthernet1/0/1: Other, IP, ARP, CDP
GigabitEthernet1/0/2: Other, IP
GigabitEthernet1/0/3: Other, IP
GigabitEthernet1/0/4: Other, IP
GigabitEthernet1/0/5: Other, IP
GigabitEthernet1/0/6: Other, IP
GigabitEthernet1/0/7: Other, IP
GigabitEthernet1/0/8: Other, IP
GigabitEthernet1/0/9: Other, IP
GigabitEthernet1/0/10: Other, IP, CDP

<output truncated>
```

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

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

<output truncated>
```

show interfaces switchport

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

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

Syntax Description	<i>interface-id</i> (Optional) ID of the interface. Valid interfaces include physical ports (including type, stack member for stacking-capable switches, module, and port number) and port channels. The port channel range is 1 to 48.				
module number	(Optional) Displays switchport configuration of all interfaces on the switch or specified stack member. This option is not available if you entered a specific interface ID.				
Command Default	None				
Command Modes	Privileged EXEC				
Command History	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; padding-bottom: 5px;">Release</th><th style="text-align: right; padding-bottom: 5px;">Modification</th></tr> </thead> <tbody> <tr> <td style="padding-bottom: 10px;">Cisco IOS XE Everest 16.6.1</td><td style="text-align: right; padding-bottom: 10px;">This command was introduced.</td></tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				

show interfaces switchport**Usage Guidelines**

Use the **show interface switchport module number** command to display the switch port characteristics of all interfaces on that switch in the stack. If there is no switch with that module number in the stack, there is no output.

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



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

```
Device# show interfaces gigabitethernet1/0/1 switchport
Name: Gi1/0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 10 (VLAN0010)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: 11-20
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

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

Field	Description
Name	Displays the port name.
Switchport	Displays the administrative and operational status of the port. In this display, the port is in switchport mode.
Administrative Mode	Displays the administrative and operational modes.
Operational Mode	
Administrative Trunking Encapsulation	Displays the administrative and operational encapsulation method and whether trunking negotiation is enabled.
Operational Trunking Encapsulation	
Negotiation of Trunking	

Field	Description
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

show interfaces transceiver

Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Examples

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

```
Device# show interfaces gigabitethernet1/1/1 transceiver detail
ITU Channel not available (Wavelength not available),
Transceiver is internally calibrated.
mA:milliamperes, dBm:decibels (milliwatts), N/A:not applicable.
++:high alarm, +:high warning, -:low warning, -- :low alarm.
A2D readouts (if they differ), are reported in parentheses.
The threshold values are uncalibrated.
```

Port	Temperature (Celsius)	High Alarm Threshold (Celsius)	High Warn Threshold (Celsius)	Low Warn Threshold (Celsius)	Low Alarm Threshold (Celsius)
Gi1/1/1	29.9	74.0	70.0	0.0	-4.0
Port	Voltage (Volts)	High Alarm Threshold (Volts)	High Warn Threshold (Volts)	Low Warn Threshold (Volts)	Low Alarm Threshold (Volts)
Gi1/1/1	3.28	3.60	3.50	3.10	3.00
Port	Optical Transmit Power (dBm)	High Alarm Threshold (dBm)	High Warn Threshold (dBm)	Low Warn Threshold (dBm)	Low Alarm Threshold (dBm)
Gi1/1/1	1.8	7.9	3.9	0.0	-4.0
Port	Optical Receive Power (dBm)	High Alarm Threshold (dBm)	High Warn Threshold (dBm)	Low Warn Threshold (dBm)	Low Alarm Threshold (dBm)
Gi1/1/1	-23.5	-5.0	-9.0	-28.2	-32.2

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

	Optical Tx	Optical Rx	Temp	Laser Bias current	Voltage
<hr/>					
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
<hr/>					
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
<hr/>					
RX only WDM GBIC					
Min1	N/A	-32.00	-4	N/A	4.65
Min2	N/A	-28.30	0	N/A	4.75

```

Max2          N/A      -9.00     70      N/A      5.25
Max1          N/A      -5.00     74      N/A      5.40
    DWDM XENPAK
Min1          -5.00    -28.00    -4      N/A      N/A
Min2          -1.00    -24.00     0      N/A      N/A
Max2          3.00     -7.00     70      N/A      N/A
Max1          7.00     -3.00     74      N/A      N/A
    DWDM X2
Min1          -5.00    -28.00    -4      N/A      N/A
Min2          -1.00    -24.00     0      N/A      N/A
Max2          3.00     -7.00     70      N/A      N/A
Max1          7.00     -3.00     74      N/A      N/A
    DWDM XFP
Min1          -5.00    -28.00    -4      N/A      N/A
Min2          -1.00    -24.00     0      N/A      N/A
Max2          3.00     -7.00     70      N/A      N/A
Max1          7.00     -3.00     74      N/A      N/A
    CWDM X2
Min1          N/A      N/A       0      N/A      N/A
Min2          N/A      N/A       0      N/A      N/A
Max2          N/A      N/A       0      N/A      N/A
Max1          N/A      N/A       0      N/A      N/A
<output truncated>

```

show inventory

To display the product inventory listing of all Cisco products installed in the networking device, use the **show inventory** command in user EXEC or privileged EXEC mode.

show inventory {fru | oid | raw} [entity]

fru	(Optional) Retrieves information about all Field Replaceable Units (FRUs) installed in the Cisco networking device.
oid	(Optional) Retrieves information about the vendor specific hardware registration identifier referred to as object identifier (OID). The OID identifies the MIB object's location in the MIB hierarchy, and provides a means of accessing the MIB object in a network of managed devices
raw	(Optional) Retrieves information about all Cisco products referred to as entities installed in the Cisco networking device, even if the entities do not have a product ID (PID) value, a unique device identifier (UDI), or other physical identification.
entity	(Optional) Name of a Cisco entity (for example, chassis, backplane, module, or slot). A quoted string may be used to display very specific UDI information; for example "sfslot 1" will display the UDI information for slot 1 of an entity named sfslot.

Command Modes Privileged EXEC (#)

Command History **Release** **Modification**

Cisco IOS XE Everest 16.6.1 This command was introduced.

show inventory**Usage Guidelines**

The **show inventory** command retrieves and displays inventory information about each Cisco product in the form of a UDI. The UDI is a combination of three separate data elements: a product identifier (PID), a version identifier (VID), and the serial number (SN).

The PID is the name by which the product can be ordered; it has been historically called the “Product Name” or “Part Number.” This is the identifier that one would use to order an exact replacement part.

The VID is the version of the product. Whenever a product has been revised, the VID will be incremented. The VID is incremented according to a rigorous process derived from Telcordia GR-209-CORE, an industry guideline that governs product change notices.

The SN is the vendor-unique serialization of the product. Each manufactured product will carry a unique serial number assigned at the factory, which cannot be changed in the field. This is the means by which to identify an individual, specific instance of a product.

The UDI refers to each product as an entity. Some entities, such as a chassis, will have subentities like slots. Each entity will display on a separate line in a logically ordered presentation that is arranged hierarchically by Cisco entities.

Use the **show inventory** command without options to display a list of Cisco entities installed in the networking device that are assigned a PID.

The following is sample output from the **show inventory** command:

```
Device# show inventory
NAME: "Chassis", DESCRIPTOR: "Cisco Catalyst 9400 Series 7 Slot Chassis"
PID: C9407R      , VID: V01 , SN: FXS2128Q13X

NAME: "Slot 2 - Linecard", DESCRIPTOR: "Cisco Catalyst 9400 Series 48-Port UPOE 10/100/1000
(RJ-45)"
PID: C9400-LC-48U      , VID: V01 , SN: JAE213102KS

NAME: "Slot 5 - Linecard", DESCRIPTOR: "Cisco Catalyst 9400 Series 48-Port UPOE 10/100/1000
(RJ-45)"
PID: C9400-LC-48U      , VID: V01 , SN: JAE2132070M

NAME: "Slot 3 - Supervisor", DESCRIPTOR: "Cisco Catalyst 9400 Series Supervisor 1 Module"
PID: C9400-SUP-1      , VID:      , SN:

NAME: "TenGigabitEthernet3/0/1", DESCRIPTOR: "10GE CU5M"
PID: N/A           , VID: T   , SN: TED2116C4SV

NAME: "Slot 4 - Supervisor", DESCRIPTOR: "Cisco Catalyst 9400 Series Supervisor 1 Module"
PID: C9400-SUP-1      , VID: V01 , SN: JAE221703LD

NAME: "TenGigabitEthernet4/0/1", DESCRIPTOR: "10GE CU5M"
PID: N/A           , VID: T   , SN: TED2116C4EG

NAME: "Power Supply Module 1", DESCRIPTOR: "Cisco Catalyst 9400 Series 3200W AC Power Supply"
PID: C9400-PWR-3200AC , VID: V01 , SN: DTM212200X2

NAME: "Fan Tray", DESCRIPTOR: "Cisco Catalyst 9400 Series 7 Slot Chassis Fan Tray"
PID: C9407-FAN      , VID: V01 , SN: FXS212206DG
```

Table 11: show inventory Field Descriptions

Field	Description
NAME	Physical name (text string) assigned to the Cisco entity. For example, console or a simple component number (port or module number), such as "1," depending on the physical component naming syntax of the device.
DESCR	Physical description of the Cisco entity that characterizes the object. The physical description includes the hardware serial number and the hardware revision.
PID	Entity product identifier. Equivalent to the entPhysicalModelName MIB variable in RFC 2737.
VID	Entity version identifier. Equivalent to the entPhysicalHardwareRev MIB variable in RFC 2737.
SN	Entity serial number. Equivalent to the entPhysicalSerialNum MIB variable in RFC 2737.

For diagnostic purposes, the **show inventory** command can be used with the **raw** keyword to display every RFC 2737 entity including those without a PID, UDI, or other physical identification.

**Note**

The **raw** keyword option is primarily intended for troubleshooting problems with the **show inventory** command itself.

Enter the **show inventory** command with an *entity* argument value to display the UDI information for a specific type of Cisco entity installed in the networking device. In this example, a list of Cisco entities that match the *sfslot* argument string is displayed. You can request even more specific UDI information with the *entity* argument value enclosed in quotation marks.

```
9407R#show inv "Slot 2 Linecard"
NAME: "Slot 2 Linecard", DESCRIPTOR: "Cisco Catalyst 9400 Series 48-Port UPOE 10/100/1000 (RJ-45)"
PID: C9400-LC-48U      , VID: V01 , SN: JAE213102KS
```

show logg onboard slot

To display the status of a line card use the **show logg onboard slot *slot-num* state** command in the global configuration mode.

show logg onboard slot *slot-num* state

Syntax Description	<i>slot-num</i>	Specifies the line card.
	state	Displays the status of the line card.
Command Default	This command has no default settings.	
Command Modes	Privileged EXEC (#)	

show memory platform

Command History	Release	Modification
	Cisco IOS XE Fuji 16.8.1a	This command was introduced.
Usage Guidelines	Use this command to monitor the state of a line card. The status is AMBER during the boot-up of the line card; RED when the linecard is disabled or has a problem; GREEN when the linecard is up and running.	

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 Everest 16.6.1	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

```

show module

```

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	<code>switch-num</code>	(Optional) Number of the switch.
Command Default	None	
Command Modes	User EXEC (>) Privileged EXEC (#)	
Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.
Usage Guidelines	Entering the show module command without the <code>switch-num</code> argument is the same as entering the show module all command.	

show mgmt-infra trace messages ilpower

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

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

Syntax Description	switch stack-member-number (Optional) Specifies the stack member number for which to display inline power messages within a trace buffer.				
Command Default	None				
Command Modes	Privileged EXEC				
Command History	<table border="1"> <thead> <tr> <th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td><td>This command was introduced.</td></tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				

This is an output example from the **show mgmt-infra trace messages ilpower** command:

```
Device# show mgmt-infra trace messages ilpower
[10/23/12 14:05:10.984 UTC 1 3] Initialized inline power system configuration fo
r slot 1.
[10/23/12 14:05:10.984 UTC 2 3] Initialized inline power system configuration fo
r slot 2.
[10/23/12 14:05:10.984 UTC 3 3] Initialized inline power system configuration fo
r slot 3.
[10/23/12 14:05:10.984 UTC 4 3] Initialized inline power system configuration fo
r slot 4.
[10/23/12 14:05:10.984 UTC 5 3] Initialized inline power system configuration fo
r slot 5.
[10/23/12 14:05:10.984 UTC 6 3] Initialized inline power system configuration fo
r slot 6.
[10/23/12 14:05:10.984 UTC 7 3] Initialized inline power system configuration fo
r slot 7.
[10/23/12 14:05:10.984 UTC 8 3] Initialized inline power system configuration fo
r slot 8.
[10/23/12 14:05:10.984 UTC 9 3] Initialized inline power system configuration fo
r slot 9.
[10/23/12 14:05:10.984 UTC a 3] Inline power subsystem initialized.
[10/23/12 14:05:18.908 UTC b 264] Create new power pool for slot 1
[10/23/12 14:05:18.909 UTC c 264] Set total inline power to 450 for slot 1
[10/23/12 14:05:20.273 UTC d 3] PoE is not supported on .
[10/23/12 14:05:20.288 UTC e 3] PoE is not supported on .
[10/23/12 14:05:20.299 UTC f 3] PoE is not supported on .
[10/23/12 14:05:20.311 UTC 10 3] PoE is not supported on .
[10/23/12 14:05:20.373 UTC 11 98] Inline power process post for switch 1
[10/23/12 14:05:20.373 UTC 12 98] PoE post passed on switch 1
[10/23/12 14:05:20.379 UTC 13 3] Slot #1: PoE initialization for board id 16387
[10/23/12 14:05:20.379 UTC 14 3] Set total inline power to 450 for slot 1
[10/23/12 14:05:20.379 UTC 15 3] Gi1/0/1 port config Initialized
[10/23/12 14:05:20.379 UTC 16 3] Interface Gi1/0/1 initialization done.
[10/23/12 14:05:20.380 UTC 17 3] Gi1/0/24 port config Initialized
[10/23/12 14:05:20.380 UTC 18 3] Interface Gi1/0/24 initialization done.
[10/23/12 14:05:20.380 UTC 19 3] Slot #1: initialization done.
[10/23/12 14:05:50.440 UTC 1a 3] Slot #1: PoE initialization for board id 16387
[10/23/12 14:05:50.440 UTC 1b 3] Duplicate init event
```

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

show mgmt-infra trace messages ilpower-ha

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

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

Syntax Description	switch <i>stack-member-number</i> (Optional) Specifies the stack member number for which to display inline power messages within a trace buffer.				
Command Default	None				
Command Modes	Privileged EXEC				
Command History	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; padding: 2px;">Release</th> <th style="text-align: left; padding: 2px;">Modification</th> </tr> </thead> <tbody> <tr> <td style="text-align: left; padding: 2px;">Cisco IOS XE Everest 16.6.1</td> <td style="text-align: left; padding: 2px;">This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				

This is an output example from the **show mgmt-infra trace messages ilpower-ha** command:

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

show mgmt-infra trace messages platform-mgr-poe

To display platform manager Power over Ethernet (PoE) messages within a trace buffer, use the **show mgmt-infra trace messages platform-mgr-poe** privileged EXEC command.

```
show mgmt-infra trace messages platform-mgr-poe [switch stack-member-number]
```

Syntax Description	switch <i>stack-member-number</i> (Optional) Specifies the stack member number for which to display messages within a trace buffer.				
Command Default	None				
Command Modes	Privileged EXEC				
Command History	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; padding: 2px;">Release</th> <th style="text-align: left; padding: 2px;">Modification</th> </tr> </thead> <tbody> <tr> <td style="text-align: left; padding: 2px;">Cisco IOS XE Everest 16.6.1</td> <td style="text-align: left; padding: 2px;">This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				

This is an example of partial output from the **show mgmt-infra trace messages platform-mgr-poe** command:

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

show network-policy profile

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

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

Syntax Description	<i>profile-number</i> (Optional) Displays the network-policy profile number. If no profile is entered, all network-policy profiles appear.				
detail	(Optional) Displays detailed status and statistics information.				
Command Default	None				
Command Modes	Privileged EXEC				
Command History	<table border="0"> <tr> <td>Release</td><td>Modification</td></tr> <tr> <td>Cisco IOS XE Everest 16.6.1</td><td>This command was introduced.</td></tr> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	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
```

show platform hardware fed active forward

```

Interface:
  none
Network Policy Profile 36
  voice vlan 4 cos 3
Interface:
  Interface_id

```

show platform hardware fed active forward

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

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

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

show platform hardware fed {active | standby} forward

Syntax Description	{ active standby } The switch for which you want to display information. You have the following options :				
	<ul style="list-style-type: none"> • active—Displays information relating to the active switch. • standby—Displays information relating to the standby switch, if available. 				
forward	Displays packet forwarding information.				
Command Modes	Privileged EXEC (#)				
Command History	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; padding-bottom: 2px;">Release</th><th style="text-align: right; padding-bottom: 2px;">Modification</th></tr> </thead> <tbody> <tr> <td style="padding-top: 2px;">Cisco IOS XE Everest 16.6.1</td><td style="text-align: right; padding-top: 2px;">This command was introduced.</td></tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				
Usage Guidelines	<p>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.</p> <p>Fields displayed in the command output are explained below.</p> <ul style="list-style-type: none"> • Station Index : The Station Index is the result of the layer 2 lookup and points to a station descriptor which provides the following: <ul style="list-style-type: none"> • Destination Index : Determines the egress port(s) to which the packets should be sent to. Global Port Number(GPN) can be used as the destination index. A destination index with 15 down to 12 bits set indicates the GPN to be used. For example, destination index - 0xF04E corresponds to GPN - 78 (0x4e). • Rewrite Index : Determines what needs to be done with the packets. For layer 2 switching, this is typically a bridging action • Flexible Lookup Pipeline Stages(FPS) : Indicates the forwarding decision that was taken for the packet - routing or bridging 				

- Replication Bit Map : Determines if the packets should be sent to CPU or stack
 - Local Data Copy = 1
 - Remote Data copy = 0
 - Local CPU Copy = 0
 - Remote CPU Copy = 0

show platform hardware iomd lc-portmap brief

To display the line card port map information of the platform, use the **show platform hardware iomd lc-portmap brief** command in privileged EXEC mode.

show platform hardware iomd slot/card lc-portmap brief

Syntax Description	<i>slot</i> Slot number. The range is from 0 to 10. <i>card</i> Card number. The range is from 0 to 0.				
Command Modes	Privileged EXEC (#)				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				

Examples

The following is sample output from the **show platform hardware iomd lc-portmap brief** command:

```
Device# show platform hardware iomd 1/0 lc-portmap brief
```

```

id 1 asic 0 port 0 intl_port_sup0 8 intl_port_sup1 0 max_speed DEV_PORT_SPEED_10G
id 2 asic 0 port 1 intl_port_sup0 8 intl_port_sup1 0 max_speed DEV_PORT_SPEED_10G
id 3 asic 0 port 2 intl_port_sup0 8 intl_port_sup1 0 max_speed DEV_PORT_SPEED_10G
id 4 asic 0 port 3 intl_port_sup0 10 intl_port_sup1 2 max_speed DEV_PORT_SPEED_10G
id 5 asic 0 port 4 intl_port_sup0 10 intl_port_sup1 2 max_speed DEV_PORT_SPEED_10G
id 6 asic 0 port 5 intl_port_sup0 10 intl_port_sup1 2 max_speed DEV_PORT_SPEED_10G
id 7 asic 1 port 6 intl_port_sup0 9 intl_port_sup1 1 max_speed DEV_PORT_SPEED_10G
id 8 asic 1 port 7 intl_port_sup0 9 intl_port_sup1 1 max_speed DEV_PORT_SPEED_10G
id 9 asic 1 port 8 intl_port_sup0 9 intl_port_sup1 1 max_speed DEV_PORT_SPEED_10G
id 10 asic 1 port 9 intl_port_sup0 10 intl_port_sup1 2 max_speed DEV_PORT_SPEED_10G
id 11 asic 1 port 10 intl_port_sup0 10 intl_port_sup1 2 max_speed DEV_PORT_SPEED_10G
id 12 asic 1 port 11 intl_port_sup0 10 intl_port_sup1 2 max_speed DEV_PORT_SPEED_10G
id 13 asic 2 port 12 intl_port_sup0 8 intl_port_sup1 0 max_speed DEV_PORT_SPEED_10G
id 14 asic 2 port 13 intl_port_sup0 8 intl_port_sup1 0 max_speed DEV_PORT_SPEED_10G
id 15 asic 2 port 14 intl_port_sup0 8 intl_port_sup1 0 max_speed DEV_PORT_SPEED_10G
id 16 asic 2 port 15 intl_port_sup0 10 intl_port_sup1 2 max_speed DEV_PORT_SPEED_10G
id 17 asic 2 port 16 intl_port_sup0 10 intl_port_sup1 2 max_speed DEV_PORT_SPEED_10G
id 18 asic 2 port 17 intl_port_sup0 10 intl_port_sup1 2 max_speed DEV_PORT_SPEED_10G
id 19 asic 3 port 18 intl_port_sup0 8 intl_port_sup1 0 max_speed DEV_PORT_SPEED_10G
id 20 asic 3 port 19 intl_port_sup0 8 intl_port_sup1 0 max_speed DEV_PORT_SPEED_10G

```

show platform hardware iomd portgroups

```

id 21 asic 3 port 20 intl_port_sup0 8 intl_port_sup1 0 max_speed DEV_PORT_SPEED_10G
id 22 asic 3 port 21 intl_port_sup0 10 intl_port_sup1 2 max_speed DEV_PORT_SPEED_10G
id 23 asic 3 port 22 intl_port_sup0 10 intl_port_sup1 2 max_speed DEV_PORT_SPEED_10G
id 24 asic 3 port 23 intl_port_sup0 10 intl_port_sup1 2 max_speed DEV_PORT_SPEED_10G

```

show platform hardware iomd portgroups

To display the port grouping information of the platform, use the **show platform hardware iomd portgroups** command in privileged EXEC mode.

show platform hardware iomd *slot/card* portgroups

Syntax Description	<i>slot</i> Slot number. The range is from 0 to 10. <i>card</i> Card number. The range is from 0 to 0.				
Command Modes	Privileged EXEC (#)				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				

Examples

The following is sample output from the **show platform hardware iomd portgroups** command:

```

Device# show platform hardware iomd 1/0 portgroups

Port      Interface                      Status    Interface  Group Max
Group

1         TenGigabitEthernet1/0/1          up       10G
1         TenGigabitEthernet1/0/2          up       10G
1         TenGigabitEthernet1/0/3          down     10G      10G

2         TenGigabitEthernet1/0/4          up       10G
2         TenGigabitEthernet1/0/5          down     10G
2         TenGigabitEthernet1/0/6          down     10G      10G

3         TenGigabitEthernet1/0/7          up       10G
3         TenGigabitEthernet1/0/8          down     10G
3         TenGigabitEthernet1/0/9          down     10G      10G

4         TenGigabitEthernet1/0/10         up       10G
4         TenGigabitEthernet1/0/11         down     10G
4         TenGigabitEthernet1/0/12         down     10G      10G

5         TenGigabitEthernet1/0/13         up       10G
5         TenGigabitEthernet1/0/14         down     10G
5         TenGigabitEthernet1/0/15         down     10G      10G

6         TenGigabitEthernet1/0/16         down     10G
6         TenGigabitEthernet1/0/17         up       10G
6         TenGigabitEthernet1/0/18         down     10G      10G

```

7	TenGigabitEthernet1/0/19	down	10G	
7	TenGigabitEthernet1/0/20	down	10G	
7	TenGigabitEthernet1/0/21	down	10G	10G
8	TenGigabitEthernet1/0/22	down	10G	
8	TenGigabitEthernet1/0/23	down	10G	
8	TenGigabitEthernet1/0/24	down	10G	10G

show platform resources

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

show platform resources

This command has no arguments or keywords.

Command Modes	Privileged EXEC (#)			
Command History	Release Modification			
	Cisco IOS XE Everest 16.6.1 This command was introduced.			
Usage Guidelines	The output of this command displays the used memory, which is total memory minus the accurate free memory.			

Example

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

```
Switch# show platform resources
**State Acronym: H - Healthy, W - Warning, C - Critical

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

show platform software ilpower

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

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

show platform software ilpower

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 Everest 16.6.1	The command was introduced.

Examples

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

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

show platform software process list

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

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

Syntax Description

switch <i>switch-number</i>	Displays information about the switch. Valid values for <i>switch-number</i> argument are from 0 to 9.
active	Displays information about the active instance of the switch.
standby	Displays information about the standby instance of the switch.
0	Displays information about the shared port adapters (SPA) Interface Processor slot 0.
F0	Displays information about the Embedded Service Processor (ESP) slot 0.
R0	Displays information about the Route Processor (RP) slot 0.
name <i>process-name</i>	(Optional) Displays information about the specified process. Enter the process name.
process-id <i>process-ID</i>	(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 Gibraltar 16.10.1	The Size column in the output was modified to display Resident Set Size (RSS) in KB.
Cisco IOS XE Everest 16.6.1	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
```

show platform software process list

```

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:

```
Device# show platform software process list switch active R0
Name          Pid   PPid  Group Id Status Priority Size
-----
systemd        1     0      1   S       20    7892
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
migration/1   10    2      0   S       4294967196 0
ksoftirqd/1   11    2      0   S       20    0
kworker/1:0H  13    2      0   S       0     0
migration/2   14    2      0   S       4294967196 0
ksoftirqd/2   15    2      0   S       20    0
kworker/2:0H  17    2      0   S       0     0
systemd-journal 221  1      221 S       20    4460
kworker/1:3   246    2      0   S       20    0
systemd-udevd 253    1      253 S       20    5648
kvm-irqfd-clean 617  2      0   S       0     0
scsi_eh_6     620    2      0   S       20    0
scsi_tmf_6    621    2      0   S       0     0
usb-storage   622    2      0   S       20    0
scsi_eh_7     625    2      0   S       20    0
scsi_tmf_7    626    2      0   S       0     0
usb-storage   627    2      0   S       20    0
kworker/7:1   630    2      0   S       20    0
bioset        631    2      0   S       0     0
kworker/3:1H  648    2      0   S       0     0
kworker/0:1H  667    2      0   S       0     0
kworker/1:1H  668    2      0   S       0     0
bioset        669    2      0   S       0     0
kworker/6:2   698    2      0   S       20    0
kworker/2:2   699    2      0   S       20    0
kworker/2:1H  703    2      0   S       0     0
kworker/7:1H  748    2      0   S       0     0
kworker/5:1H  749    2      0   S       0     0
kworker/6:1H  754    2      0   S       0     0
kworker/7:2   779    2      0   S       20    0
auditd       838    1      838 S       16    2564
.
.
.
```

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

Table 12: 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

show platform software process slot switch

Field	Description
Status	Displays the process status in human readable form.
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 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-times	(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
	This command was introduced.
Usage Guidelines	<p>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.</p>
Examples	<p>The following is sample output from the show platform software process slot switch active R0 monitor command:</p>
<pre>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 S 0 0.0 0:00.00 kthreadd 3 root 20 0 0 0 S 0 0.0 0:02.86 ksoftirqd/0 5 root 0 -20 0 0 S 0 0.0 0:00.00 kworker/0:0H 7 root RT 0 0 0 S 0 0.0 0:01.44 migration/0 8 root 20 0 0 0 S 0 0.0 0:00.00 rcu_bh 9 root 20 0 0 0 S 0 0.0 0:23.08 rcu_sched 10 root 20 0 0 0 S 0 0.0 0:58.04 rcuc/0 11 root 20 0 0 0 S 0 0.0 21:35.60 rcuc/1 12 root RT 0 0 0 S 0 0.0 0:01.33 migration/1</pre>	

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}]

show platform software status control-processor

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

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

Command History	Release	Modification
------------------------	----------------	---------------------

Cisco IOS XE Everest 16.6.1 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)

```

show processes cpu platform monitor

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
	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
	0	3.99	0.69	0.00	95.30	0.00	0.00	0.00
	1	2.60	0.70	0.00	96.70	0.00	0.00	0.00
	2	4.49	0.89	0.00	94.60	0.00	0.00	0.00
	3	2.60	0.20	0.00	97.20	0.00	0.00	0.00

show processes cpu platform monitor

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

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

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

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.
Usage Guidelines	<p>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.</p>	
Examples	<p>The following is sample output from the show processes cpu monitor location switch active R0 command:</p> <pre>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</pre>	

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

show processes memory platform

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

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

show processes memory platform

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

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

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	The command was introduced.

Examples

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

```
Switch# show processes memory platform
```

```
System memory: 3976852K total, 2761580K used, 1215272K free,
Lowest: 1215272K
      Pid   Text     Data   Stack   Dynamic      RSS      Total           Name
-----+
      1   1246    4400    132    1308    4400    8328           systemd
     96   233     2796    132     132    2796   12436  systemd-journal
    105   284     1796    132     176    1796    5208  systemd-udevd
    707    52     2660    132     172    2660   11688          in.telnetd
    744   968     3264    132    1700    3264    5800       brelay.sh
    835    52     2660    132     172    2660   11688  in.telnetd
    863   968     3264    132    1700    3264    5800       brelay.sh
```

```

928      968      3996      132      2312      3996      6412      reflector.sh
933      968      3976      132      2312      3976      6412      droputil.sh
934      968      2140      132      528       2140      4628      oom.sh
936      173       936      132      132       936      3068      xinetd
945      968      1472      132      132       1472      4168      libvirttd.sh
947      592      43164     132      3096      43164     154716     repm
954      45        932      132      132       932       3132      rpcbind
986      482      3476      132      132       3476     169288     libvirttd
988      66        940      132      132       940       2724      rpc.statd
993      968      928       132      132       928       4232      boothelper_evt.
1017     21        640      132      132       640       2500      inotifywait
1089     102      1200      132      132       1200      3328      rpc.mountd
1328      9        2940      132      148       2940     13844      rotee
1353     39        532      132      132       532       2336      sleep
!
!
!
```

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

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

```

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

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

```
Switch# show processes memory platform sorted
```

```

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

show system mtu

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

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

```
System memory: 3976852K total, 2763584K used, 1213268K free,
Lowest: 1213268K
```

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

show 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 Everest 16.6.1	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:	

show tech-support

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

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

Syntax Description		
cef	(Optional) Displays CEF related information.	
cft	(Optional) Displays CFT related information.	
eigrp	(Optional) Displays EIGRP related information.	
evc	(Optional) Displays EVC related information.	
fnf	(Optional) Displays flexible netflow related information.	
ipc	(Optional) Displays IPC related information.	
ipmulticast	(Optional) Displays IP multicast related information.	
ipsec	(Optional) Displays IPSEC related information.	
mfib	(Optional) Displays MFIB related information.	
nat	(Optional) Displays NAT related information.	
nbar	(Optional) Displays NBAR related information.	
onep	(Optional) Displays ONEP related information.	
ospf	(Optional) Displays OSPF related information.	
page	(Optional) Displays the command output on a single page at a time. Use the Return key to display the next line of output or use the space bar to display the next page of information. If not used, the output scrolls (that is, it does not stop for page breaks). Press the Ctrl-C keys to stop the command output.	
password	(Optional) Leaves passwords and other security information in the output. If not used, passwords and other security-sensitive information in the output are replaced with the label "<removed>".	
rsvp	(Optional) Displays IP RSVP related information.	
subscriber	(Optional) Displays subscriber related information.	
vrrp	(Optional) Displays VRRP related information.	
wccp	(Optional) Displays WCCP related information.	
Command Modes	Privileged EXEC (#)	
Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.10.1	This command was enhanced to display the output of the show logging onboard uptime command

speed

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was implemented on the Cisco Catalyst 9400 Series Switches

Usage Guidelines

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

You can use one of the following redirection methods:

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

speed

To specify the speed of a 10/100/1000/2500/5000 Mbps port, use the **speed** command in interface configuration mode. To return to the default value, use the **no** form of this command.

```
speed {10 | 100 | 1000 | 2500 | 5000 | auto [{10 | 100 | 1000 | 2500 | 5000}] | nonegotiate}
no speed
```

Syntax Description

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

Command Default

The default is **auto**.

Command Modes

Interface configuration

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	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 new keywords, 2500 and 5000 are visible only on multi-Gigabit (m-Gig) Ethernet supporting devices.		
If the speed is set to auto , the switch negotiates with the device at the other end of the link for the speed setting, and then forces the speed setting to the negotiated value. The duplex setting remains configured on each end of the link, which might result in a duplex setting mismatch.		
If both ends of the line support autonegotiation, we highly recommend the default autonegotiation settings. If one interface supports autonegotiation and the other end does not, use the auto setting on the supported side, but set the duplex and speed on the other side.		
		
Caution		Changing the interface speed and duplex mode configuration might shut down and re-enable the interface during the reconfiguration.
For guidelines on setting the switch speed and duplex parameters, see the “Configuring Interface Characteristics” chapter in the software configuration guide for this release.		
Verify your settings using the show interfaces privileged EXEC command.		
Examples		The following example shows how to set speed on a port to 100 Mbps:
<pre>Device(config)# interface gigabitethernet1/0/1 Device(config-if)# speed 100</pre>		
The following example shows how to set a port to autonegotiate at only 10 Mbps:		
<pre>Device(config)# interface gigabitethernet1/0/1 Device(config-if)# speed auto 10</pre>		
The following example shows how to set a port to autonegotiate at only 10 or 100 Mbps:		
<pre>Device(config)# interface gigabitethernet1/0/1 Device(config-if)# speed auto 10 100</pre>		

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}
```

system mtu

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.				
Command Default	Unknown multicast and unicast traffic is not blocked.				
Command Modes	Interface configuration				
Command History	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; padding-bottom: 5px;">Release</th><th style="text-align: right; padding-bottom: 5px;">Modification</th></tr> </thead> <tbody> <tr> <td style="padding-top: 5px;">Cisco IOS XE Everest 16.6.1</td><td style="text-align: right; padding-top: 5px;">This command was introduced.</td></tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				
Usage Guidelines	<p>By default, all traffic with unknown MAC addresses is sent to all ports. You can block unknown multicast or unicast traffic on protected or nonprotected ports. If unknown multicast or unicast traffic is not blocked on a protected port, there could be security issues.</p> <p>With multicast traffic, the port blocking feature blocks only pure Layer 2 packets. Multicast packets that contain IPv4 or IPv6 information in the header are not blocked.</p> <p>Blocking unknown multicast or unicast traffic is not automatically enabled on protected ports; you must explicitly configure it.</p> <p>For more information about blocking packets, see the software configuration guide for this release.</p> <p>This example shows how to block unknown unicast traffic on an interface:</p> <pre>Device(config-if)# switchport block unicast</pre> <p>You can verify your setting by entering the show interfaces <i>interface-id</i> switchport privileged EXEC command.</p>				

system mtu

Syntax Description	<i>bytes</i>				
Command Default	The default MTU size for all ports is 1500 bytes.				
Command Modes	Global configuration				
Command History	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; padding-bottom: 5px;">Release</th><th style="text-align: right; padding-bottom: 5px;">Modification</th></tr> </thead> <tbody> <tr> <td style="padding-top: 5px;">Cisco IOS XE Everest 16.6.1</td><td style="text-align: right; padding-top: 5px;">This command was introduced.</td></tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				
Usage Guidelines	<p>You can verify your setting by entering the show system mtu privileged EXEC command.</p> <p>The switch does not support the MTU on a per-interface basis.</p>				

If you enter a value that is outside the allowed range for the specific type of interface, the value is not accepted.

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	<p>vlan-id (Optional) The VLAN for voice traffic. The range is 1 to 4094.</p> <p>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.</p> <p>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.</p> <p>dot1p (Optional) Configures the phone to use IEEE 802.1p priority tagging and to use VLAN 0 (the native VLAN).</p> <p>none (Optional) Does not instruct the Cisco IP phone about the voice VLAN. The phone uses the configuration from the phone key pad.</p> <p>untagged (Optional) Configures the phone to send untagged voice traffic. This is the default for the phone.</p>
---------------------------	---

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 Everest 16.6.1	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.

voice vlan (network-policy configuration)

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

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

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

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

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

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

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

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

voice vlan (network-policy configuration)

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

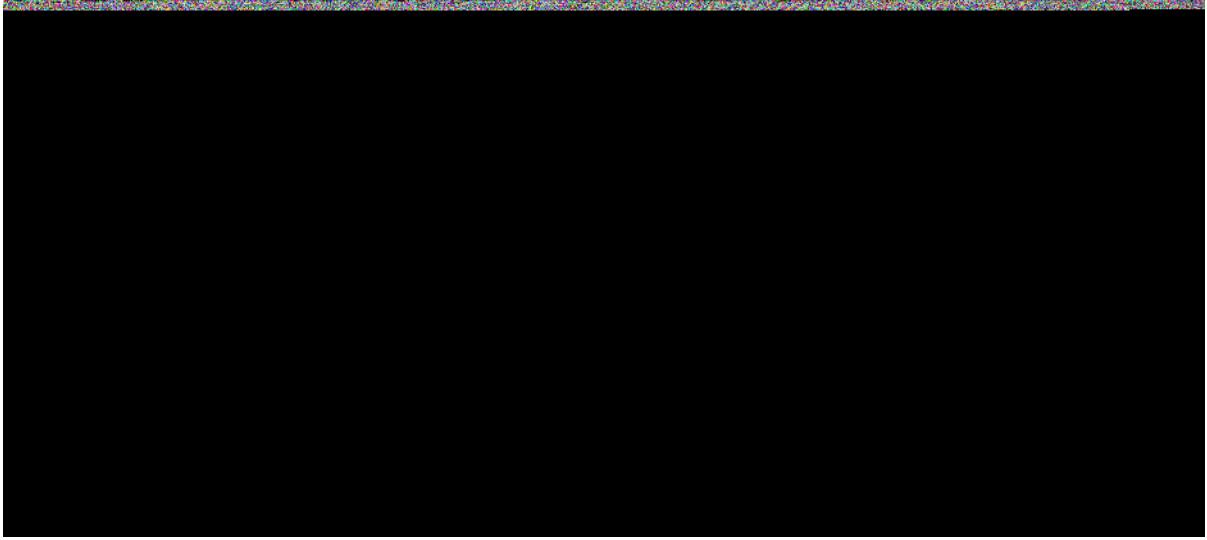
```
voice vlan {vlan-id [{cos cos-value | dscp dscp-value}] | dot1p [{cos l2-priority | dscp dscp}] | none | untagged}
```

Syntax Description	<p>vlan-id (Optional) The VLAN for voice traffic. The range is 1 to 4094.</p> <p>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.</p> <p>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.</p> <p>dot1p (Optional) Configures the phone to use IEEE 802.1p priority tagging and to use VLAN 0 (the native VLAN).</p> <p>none (Optional) Does not instruct the Cisco IP phone about the voice VLAN. The phone uses the configuration from the phone key pad.</p> <p>untagged (Optional) Configures the phone to send untagged voice traffic. This is the default for the phone.</p>
---------------------------	---

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 Everest 16.6.1	This command was introduced.
Usage Guidelines	<p>Use the network-policy profile global configuration command to create a profile and to enter network-policy profile configuration mode.</p> <p>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.</p> <p>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.</p> <p>These profile attributes are contained in the Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED) network-policy time-length-value (TLV).</p> <p>To return to privileged EXEC mode from the network-policy profile configuration mode, enter the exit command.</p>	
	<p>This example shows how to configure the voice application type for VLAN 100 with a priority 4 CoS:</p> <pre>Device(config)# network-policy profile 1 Device(config-network-policy)# voice vlan 100 cos 4</pre> <p>This example shows how to configure the voice application type for VLAN 100 with a DSCP value of 34:</p> <pre>Device(config)# network-policy profile 1 Device(config-network-policy)# voice vlan 100 dscp 34</pre> <p>This example shows how to configure the voice application type for the native VLAN with priority tagging:</p> <pre>Device(config-network-policy)# voice vlan dot1p cos 4</pre>	

voice vlan (network-policy configuration)



PART IV

IP Addressing Services

- IP Addressing Services Commands, on page 181

CHAPTER ■

IP Addressing Services Commands

- [clear ip nhrp](#), on page 181
- [debug nhrp](#), on page 182
- [fhrp delay](#), on page 184
- [fhrp version vrrp v3](#), on page 185
- [ip address](#), on page 185
- [ip address dhcp](#), on page 188
- [ip address pool \(DHCP\)](#), on page 190
- [ip nhrp map](#), on page 191
- [ip nhrp map multicast](#), on page 192
- [ip nhrp network-id](#), on page 193
- [ip nhrp nhs](#), on page 194
- [ipv6 nd cache expire](#), on page 196
- [ipv6 nd na glean](#), on page 197
- [ipv6 nd nud retry](#), on page 197
- [key chain](#), on page 199
- [key-string \(authentication\)](#), on page 200
- [key](#) , on page 201
- [show ip nhrp nhs](#), on page 201
- [show ip ports all](#), on page 203
- [show key chain](#), on page 205
- [show track](#), on page 205
- [track](#), on page 207
- [vrrp](#), on page 208
- [vrrp description](#), on page 209
- [vrrp preempt](#), on page 210
- [vrrp priority](#), on page 211
- [vrrp timers advertise](#), on page 211
- [vrrs leader](#), on page 212

clear ip nhrp

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

debug nhrp

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

Syntax Description	<table border="1"> <tr> <td>vrf</td><td>(Optional) Deletes entries from the NHRP cache for the specified virtual routing and forwarding (VRF) instance.</td></tr> <tr> <td><i>vrf-name</i></td><td>(Optional) Name of the VRF address family to which the command is applied.</td></tr> <tr> <td>global</td><td>(Optional) Specifies the global VRF instance.</td></tr> <tr> <td><i>dest-ip-address</i></td><td>(Optional) Destination IP address. Specifying this argument clears NHRP mapping entries for the specified destination IP address.</td></tr> <tr> <td><i>dest-mask</i></td><td>(Optional) Destination network mask.</td></tr> <tr> <td>counters</td><td>(Optional) Clears the NHRP counters.</td></tr> <tr> <td>interface</td><td>(Optional) Clears the NHRP mapping entries for all interfaces.</td></tr> <tr> <td>tunnel number</td><td>(Optional) Removes the specified interface from the NHRP cache.</td></tr> <tr> <td>stats</td><td>(Optional) Clears all IPv4 statistic information for all interfaces.</td></tr> </table>	vrf	(Optional) Deletes entries from the NHRP cache for the specified virtual routing and forwarding (VRF) instance.	<i>vrf-name</i>	(Optional) Name of the VRF address family to which the command is applied.	global	(Optional) Specifies the global VRF instance.	<i>dest-ip-address</i>	(Optional) Destination IP address. Specifying this argument clears NHRP mapping entries for the specified destination IP address.	<i>dest-mask</i>	(Optional) Destination network mask.	counters	(Optional) Clears the NHRP counters.	interface	(Optional) Clears the NHRP mapping entries for all interfaces.	tunnel number	(Optional) Removes the specified interface from the NHRP cache.	stats	(Optional) Clears all IPv4 statistic information for all interfaces.
vrf	(Optional) Deletes entries from the NHRP cache for the specified virtual routing and forwarding (VRF) instance.																		
<i>vrf-name</i>	(Optional) Name of the VRF address family to which the command is applied.																		
global	(Optional) Specifies the global VRF instance.																		
<i>dest-ip-address</i>	(Optional) Destination IP address. Specifying this argument clears NHRP mapping entries for the specified destination IP address.																		
<i>dest-mask</i>	(Optional) Destination network mask.																		
counters	(Optional) Clears the NHRP counters.																		
interface	(Optional) Clears the NHRP mapping entries for all interfaces.																		
tunnel number	(Optional) Removes the specified interface from the NHRP cache.																		
stats	(Optional) Clears all IPv4 statistic information for all interfaces.																		

Command Modes User EXEC (>)

Privileged EXEC (#)

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

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

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

```
Switch# clear ip nhrp
```

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

debug nhrp

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

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

Syntax Description	<table border="1"> <tr> <td>attribute</td><td>(Optional) Enables NHRP attribute debugging operations.</td></tr> <tr> <td>cache</td><td>(Optional) Enables NHRP cache debugging operations.</td></tr> <tr> <td>condition</td><td>(Optional) Enables NHRP conditional debugging operations.</td></tr> <tr> <td>interface tunnel <i>number</i></td><td>(Optional) Enables debugging operations for the tunnel interface.</td></tr> <tr> <td>nbma</td><td>(Optional) Enables debugging operations for the non-broadcast multiple access (NBMA) network.</td></tr> <tr> <td><i>ipv4-nbma-address</i></td><td>(Optional) Enables debugging operations based on the IPv4 address of the NBMA network.</td></tr> <tr> <td><i>nbma-name</i></td><td>(Optional) NBMA network name.</td></tr> <tr> <td><i>IPv6-address</i></td><td>(Optional) Enables debugging operations based on the IPv6 address of the NBMA network. Note The <i>IPv6-address</i> argument is not supported in Cisco IOS XE Denali 16.3.1.</td></tr> <tr> <td>vrf <i>vrf-name</i></td><td>(Optional) Enables debugging operations for the virtual routing and forwarding instance.</td></tr> <tr> <td>detail</td><td>(Optional) Displays detailed logs of NHRP debugs.</td></tr> <tr> <td>error</td><td>(Optional) Enables NHRP error debugging operations.</td></tr> <tr> <td>extension</td><td>(Optional) Enables NHRP extension processing debugging operations.</td></tr> <tr> <td>group</td><td>(Optional) Enables NHRP group debugging operations.</td></tr> <tr> <td>packet</td><td>(Optional) Enables NHRP activity debugging.</td></tr> <tr> <td>rate</td><td>(Optional) Enables NHRP rate limiting.</td></tr> <tr> <td>routing</td><td>(Optional) Enables NHRP routing debugging operations.</td></tr> </table>	attribute	(Optional) Enables NHRP attribute debugging operations.	cache	(Optional) Enables NHRP cache debugging operations.	condition	(Optional) Enables NHRP conditional debugging operations.	interface tunnel <i>number</i>	(Optional) Enables debugging operations for the tunnel interface.	nbma	(Optional) Enables debugging operations for the non-broadcast multiple access (NBMA) network.	<i>ipv4-nbma-address</i>	(Optional) Enables debugging operations based on the IPv4 address of the NBMA network.	<i>nbma-name</i>	(Optional) NBMA network name.	<i>IPv6-address</i>	(Optional) Enables debugging operations based on the IPv6 address of the NBMA network. Note The <i>IPv6-address</i> argument is not supported in Cisco IOS XE Denali 16.3.1.	vrf <i>vrf-name</i>	(Optional) Enables debugging operations for the virtual routing and forwarding instance.	detail	(Optional) Displays detailed logs of NHRP debugs.	error	(Optional) Enables NHRP error debugging operations.	extension	(Optional) Enables NHRP extension processing debugging operations.	group	(Optional) Enables NHRP group debugging operations.	packet	(Optional) Enables NHRP activity debugging.	rate	(Optional) Enables NHRP rate limiting.	routing	(Optional) Enables NHRP routing debugging operations.
attribute	(Optional) Enables NHRP attribute debugging operations.																																
cache	(Optional) Enables NHRP cache debugging operations.																																
condition	(Optional) Enables NHRP conditional debugging operations.																																
interface tunnel <i>number</i>	(Optional) Enables debugging operations for the tunnel interface.																																
nbma	(Optional) Enables debugging operations for the non-broadcast multiple access (NBMA) network.																																
<i>ipv4-nbma-address</i>	(Optional) Enables debugging operations based on the IPv4 address of the NBMA network.																																
<i>nbma-name</i>	(Optional) NBMA network name.																																
<i>IPv6-address</i>	(Optional) Enables debugging operations based on the IPv6 address of the NBMA network. Note The <i>IPv6-address</i> argument is not supported in Cisco IOS XE Denali 16.3.1.																																
vrf <i>vrf-name</i>	(Optional) Enables debugging operations for the virtual routing and forwarding instance.																																
detail	(Optional) Displays detailed logs of NHRP debugs.																																
error	(Optional) Enables NHRP error debugging operations.																																
extension	(Optional) Enables NHRP extension processing debugging operations.																																
group	(Optional) Enables NHRP group debugging operations.																																
packet	(Optional) Enables NHRP activity debugging.																																
rate	(Optional) Enables NHRP rate limiting.																																
routing	(Optional) Enables NHRP routing debugging operations.																																

Command Default NHRP debugging is not enabled.

Command Modes Privileged EXEC (#)

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

fhrp delay**Usage Guidelines**

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

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

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

Examples

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

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

Related Commands

Command	Description
show ip nhrp	Displays NHRP mapping information.

fhrp delay

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

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

Syntax Description

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

Command Default

None

Command Modes

Interface configuration (config-if)

Examples

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

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

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

fhrp version vrrp v3

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

```
fhrp version vrrp v3
no fhrp version vrrp v3
```

Syntax Description This command has no keywords or arguments.

Command Default VRRPv3 and VRRS configuration on a device is not enabled.

Command Modes Global configuration (config)

Usage Guidelines When VRRPv3 is in use, VRRP version 2 (VRRPv2) is unavailable.

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

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

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

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]]
```

ip address

Syntax Description	<table border="1"> <tr> <td><i>ip-address</i></td><td>IP address.</td></tr> <tr> <td><i>mask</i></td><td>Mask for the associated IP subnet.</td></tr> <tr> <td>secondary</td><td>(Optional) Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address. Note If the secondary address is used for a VRF table configuration with the vrf keyword, the vrf keyword must be specified also.</td></tr> <tr> <td>vrf</td><td>(Optional) Name of the VRF table. The <i>vrf-name</i> argument specifies the VRF name of the ingress interface.</td></tr> </table>	<i>ip-address</i>	IP address.	<i>mask</i>	Mask for the associated IP subnet.	secondary	(Optional) Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address. Note If the secondary address is used for a VRF table configuration with the vrf keyword, the vrf keyword must be specified also.	vrf	(Optional) Name of the VRF table. The <i>vrf-name</i> argument specifies the VRF name of the ingress interface.
<i>ip-address</i>	IP address.								
<i>mask</i>	Mask for the associated IP subnet.								
secondary	(Optional) Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address. Note If the secondary address is used for a VRF table configuration with the vrf keyword, the vrf keyword must be specified also.								
vrf	(Optional) Name of the VRF table. The <i>vrf-name</i> argument specifies the VRF name of the ingress interface.								

Command Default No IP address is defined for the interface.

Command Modes Interface configuration (config-if)

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines An interface can have one primary IP address and multiple secondary IP addresses. Packets generated by the Cisco IOS software always use the primary IP address. Therefore, all devices and access servers on a segment should share the same primary network number.

Hosts can determine subnet masks using the Internet Control Message Protocol (ICMP) mask request message. Devices respond to this request with an ICMP mask reply message.

You can disable IP processing on a particular interface by removing its IP address with the **no ip address** command. If the software detects another host using one of its IP addresses, it will print an error message on the console.

The optional **secondary** keyword allows you to specify an unlimited number of secondary addresses. Secondary addresses are treated like primary addresses, except the system never generates datagrams other than routing updates with secondary source addresses. IP broadcasts and Address Resolution Protocol (ARP) requests are handled properly, as are interface routes in the IP routing table.

Secondary IP addresses can be used in a variety of situations. The following are the most common applications:

- There may not be enough host addresses for a particular network segment. For example, your subnetting allows up to 254 hosts per logical subnet, but on one physical subnet you need 300 host addresses. Using secondary IP addresses on the devices or access servers allows you to have two logical subnets using one physical subnet.
- Many older networks were built using Level 2 bridges. The judicious use of secondary addresses can aid in the transition to a subnetted, device-based network. Devices on an older, bridged segment can be easily made aware that many subnets are on that segment.
- Two subnets of a single network might otherwise be separated by another network. This situation is not permitted when subnets are in use. In these instances, the first network is *extended*, or layered on top of the second network using secondary addresses.

**Note**

- If any device on a network segment uses a secondary address, all other devices on that same segment must also use a secondary address from the same network or subnet. Inconsistent use of secondary addresses on a network segment can very quickly cause routing loops.
- 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.

To transparently bridge IP on an interface, you must perform the following two tasks:

- Disable IP routing (specify the **no ip routing** command).
- Add the interface to a bridge group, see the **bridge-group** command.

To concurrently route and transparently bridge IP on an interface, see the **bridge crb** command.

Examples

In the following example, 192.108.1.27 is the primary address and 192.31.7.17 is the secondary address for GigabitEthernet interface 1/0/1:

```
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 address dhcp

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)

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 13: Configuration Method and Resulting Contents of the DISCOVER Message

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

Examples

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

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

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

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

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

```
hostname abc
!
```

ip address pool (DHCP)

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

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

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

Related Commands

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

ip address pool (DHCP)

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

```
ip address pool name
no ip address pool
```

Syntax Description

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

Command Default

IP address pooling is disabled.

Command Modes

Interface configuration

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 nhrp map

To statically configure the IP-to-nonbroadcast multiaccess (NBMA) address mapping of IP destinations connected to an NBMA network, use the **ip nhrp map** interface configuration command. To remove the static entry from Next Hop Resolution Protocol (NHRP) cache, use the **no** form of this command.

```
ip nhrp map {ip-address [nbma-ip-address][dest-mask][nbma-ipv6-address] | multicast
{nbma-ip-address nbma-ipv6-address | dynamic}}
no ip nhrp map {ip-address [nbma-ip-address][dest-mask][nbma-ipv6-address] | multicast
{nbma-ip-address nbma-ipv6-address | dynamic}}
```

Syntax Description	<i>ip-address</i>	IP address of the destinations reachable through the Nonbroadcast multiaccess (NBMA) network. This address is mapped to the NBMA address.
	<i>nbma-ip-address</i>	NBMA IP address.
	<i>dest-mask</i>	Destination network address for which a mask is required.
	<i>nbma-ipv6-address</i>	NBMA IPv6 address.
	dynamic	Dynamically learns destinations from client registrations on hub.
	multicast	NBMA address that is directly reachable through the NBMA network. The address format varies depending on the medium you are using. For example, ATM has a Network Service Access Point (NSAP) address, Ethernet has a MAC address, and Switched Multimegabit Data Service (SMDS) has an E.164 address. This address is mapped to the IP address.

Command Default No static IP-to-NBMA cache entries exist.

Command Modes Interface configuration (config-if)

Command History	Release	Modification
		This command was introduced.

Usage Guidelines You will probably need to configure at least one static mapping in order to reach the next-hop server. Repeat this command to statically configure multiple IP-to-NBMA address mappings.

Examples In the following example, this station in a multipoint tunnel network is statically configured to be served by two next-hop servers 10.0.0.1 and 10.0.1.3. The NBMA address for 10.0.0.1 is statically configured to be 192.0.0.1 and the NBMA address for 10.0.1.3 is 192.2.7.8.

```
Device(config)# interface tunnel 0
Device(config-if)# ip nhrp nhs 10.0.0.1
```

ip nhrp map multicast

```
Device(config-if)# ip nhrp nhs 10.0.1.3
Device(config-if)# ip nhrp map 10.0.0.1 192.0.0.1
Device(config-if)# ip nhrp map 10.0.1.3 192.2.7.8
```

Examples

In the following example, if a packet is sent to 10.255.255.255, it is replicated to destinations 10.0.0.1 and 10.0.0.2. Addresses 10.0.0.1 and 10.0.0.2 are the IP addresses of two other routers that are part of the tunnel network, but those addresses are their addresses in the underlying network, not the tunnel network. They would have tunnel addresses that are in network 10.0.0.0.

```
Device(config)# interface tunnel 0
Device(config-if)# ip address 10.0.0.3 255.0.0.0
Device(config-if)# ip nhrp map multicast 10.0.0.1
Device(config-if)# ip nhrp map multicast 10.0.0.2
```

Related Commands

Command	Description
clear ip nhrp	Clears all dynamic entries from the NHRP cache.

ip nhrp map multicast

To configure nonbroadcast multiaccess (NBMA) addresses used as destinations for broadcast or multicast packets to be sent over a tunnel network, use the **ip nhrp map multicast** command in interface configuration mode. To remove the destinations, use the **no** form of this command.

```
ip nhrp map multicast {ip-nbma-address ipv6-nbma-address | dynamic}
no ip nhrp map multicast {ip-nbma-address ipv6-nbma-address | dynamic}
```

Syntax Description

<i>ip-nbma-address</i>	NBMA address that is directly reachable through the NBMA network. The address format varies depending on the medium that you are using.
<i>ipv6-nbma-address</i>	IPv6 NBMA address. Note This argument is not supported in Cisco IOS XE Denali 16.3.1.
dynamic	Dynamically learns destinations from client registrations on the hub.

Command Default

No NBMA addresses are configured as destinations for broadcast or multicast packets.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

Note In Cisco IOS XE Denali 16.3.1, this command supports only IPv4; the *ipv6-nbma-address* argument although available on the switch, will not work if configured.

This command applies only to tunnel interfaces. This command is useful for supporting broadcasts over a tunnel network when the underlying network does not support IP multicast. If the underlying network does support IP multicast, you should use the **tunnel destination** command to configure a multicast destination for transmission of tunnel broadcasts or multicasts.

When multiple NBMA addresses are configured, the system replicates the broadcast packet for each address.

Examples

In the following example, if a packet is sent to 10.255.255.255, it is replicated to destinations 10.0.0.1 and 10.0.0.2:

```
Switch(config)# interface tunnel 0
Switch(config-if)# ip address 10.0.0.3 255.0.0.0
Switch(config-if)# ip nhrp map multicast 10.0.0.1
Switch(config-if)# ip nhrp map multicast 10.0.0.2
```

Related Commands

Command	Description
debug nhrp	Enables NHRP debugging.
interface	Configures an interface and enters interface configuration mode.
tunnel destination	Specifies the destination for a tunnel interface.

ip nhrp network-id

To enable the Next Hop Resolution Protocol (NHRP) on an interface, use the **ip nhrp network-id** command in interface configuration mode. To disable NHRP on the interface, use the **no** form of this command.

```
ip nhrp network-id number
no ip nhrp network-id [number]
```

Syntax Description

<i>number</i>	Globally unique, 32-bit network identifier from a nonbroadcast multiaccess (NBMA) network. The range is from 1 to 4294967295.
---------------	---

Command Default

NHRP is disabled on the interface.

Command Modes

Interface configuration (config-if)

ip nhrp nhs

Command History	Release	Modification																						
		This command was introduced.																						
Usage Guidelines	In general, all NHRP stations within one logical NBMA network must be configured with the same network identifier.																							
Examples	The following example enables NHRP on the interface:																							
<pre>Device(config-if)# ip nhrp network-id 1</pre>																								
<h2>ip nhrp nhs</h2> <p>To specify the address of one or more Next Hop Resolution Protocol (NHRP) servers, use the ip nhrp nhs command in interface configuration mode. To remove the address, use the no form of this command.</p>																								
<pre>ip nhrp nhs {nhs-address [nbma {nbma-addressFQDN-string}] [multicast] [priority value] [cluster value] cluster value max-connections value dynamic nbma {nbma-addressFQDN-string} [multicast] [priority value] [cluster value]} no ip nhrp nhs {nhs-address [nbma {nbma-addressFQDN-string}] [multicast] [priority value] [cluster value] cluster value max-connections value dynamic nbma {nbma-addressFQDN-string} [multicast] [priority value] [cluster value]}</pre>																								
Syntax Description	<table border="1"> <tbody> <tr> <td><i>nhs-address</i></td><td>Address of the next-hop server being specified.</td></tr> <tr> <td><i>net-address</i></td><td>(Optional) IP address of a network served by the next-hop server.</td></tr> <tr> <td><i>netmask</i></td><td>(Optional) IP network mask to be associated with the IP address. The IP address is logically ANDed with the mask.</td></tr> <tr> <td>nbma</td><td>(Optional) Specifies the nonbroadcast multiple access (NBMA) address or FQDN.</td></tr> <tr> <td><i>nbma-address</i></td><td>NBMA address.</td></tr> <tr> <td><i>FQDN-string</i></td><td>Next hop server (NHS) fully qualified domain name (FQDN) string.</td></tr> <tr> <td>multicast</td><td>(Optional) Specifies to use NBMA mapping for broadcasts and multicasts.</td></tr> <tr> <td>priority value</td><td>(Optional) Assigns a priority to hubs to control the order in which spokes select hubs to establish tunnels. The range is from 0 to 255; 0 is the highest and 255 is the lowest priority.</td></tr> <tr> <td>cluster value</td><td>(Optional) Specifies NHS groups. The range is from 0 to 10; 0 is the highest and 10 is the lowest. The default value is 0.</td></tr> <tr> <td>max-connections value</td><td>Specifies the number of NHS elements from each NHS group that needs to be active. The range is from 0 to 255.</td></tr> <tr> <td>dynamic</td><td>Configures the spoke to learn the NHS protocol address dynamically.</td></tr> </tbody> </table>		<i>nhs-address</i>	Address of the next-hop server being specified.	<i>net-address</i>	(Optional) IP address of a network served by the next-hop server.	<i>netmask</i>	(Optional) IP network mask to be associated with the IP address. The IP address is logically ANDed with the mask.	nbma	(Optional) Specifies the nonbroadcast multiple access (NBMA) address or FQDN.	<i>nbma-address</i>	NBMA address.	<i>FQDN-string</i>	Next hop server (NHS) fully qualified domain name (FQDN) string.	multicast	(Optional) Specifies to use NBMA mapping for broadcasts and multicasts.	priority value	(Optional) Assigns a priority to hubs to control the order in which spokes select hubs to establish tunnels. The range is from 0 to 255; 0 is the highest and 255 is the lowest priority.	cluster value	(Optional) Specifies NHS groups. The range is from 0 to 10; 0 is the highest and 10 is the lowest. The default value is 0.	max-connections value	Specifies the number of NHS elements from each NHS group that needs to be active. The range is from 0 to 255.	dynamic	Configures the spoke to learn the NHS protocol address dynamically.
<i>nhs-address</i>	Address of the next-hop server being specified.																							
<i>net-address</i>	(Optional) IP address of a network served by the next-hop server.																							
<i>netmask</i>	(Optional) IP network mask to be associated with the IP address. The IP address is logically ANDed with the mask.																							
nbma	(Optional) Specifies the nonbroadcast multiple access (NBMA) address or FQDN.																							
<i>nbma-address</i>	NBMA address.																							
<i>FQDN-string</i>	Next hop server (NHS) fully qualified domain name (FQDN) string.																							
multicast	(Optional) Specifies to use NBMA mapping for broadcasts and multicasts.																							
priority value	(Optional) Assigns a priority to hubs to control the order in which spokes select hubs to establish tunnels. The range is from 0 to 255; 0 is the highest and 255 is the lowest priority.																							
cluster value	(Optional) Specifies NHS groups. The range is from 0 to 10; 0 is the highest and 10 is the lowest. The default value is 0.																							
max-connections value	Specifies the number of NHS elements from each NHS group that needs to be active. The range is from 0 to 255.																							
dynamic	Configures the spoke to learn the NHS protocol address dynamically.																							

Command Default	No next-hop servers are explicitly configured, so normal network layer routing decisions are used to forward NHRP traffic.				
Command Modes	Interface configuration (config-if)				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td></td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification		This command was introduced.
Release	Modification				
	This command was introduced.				

Usage Guidelines Use the **ip nhrp nhs** command to specify the address of a next hop server and the networks it serves. Normally, NHRP consults the network layer forwarding table to determine how to forward NHRP packets. When next hop servers are configured, these next hop addresses override the forwarding path that would otherwise be used for NHRP traffic.

When the **ip nhrp nhs dynamic** command is configured on a DMVPN tunnel and the **shut** command is issued to the tunnel interface, the crypto socket does not receive shut message, thereby not bringing up a DMVPN session with the hub.

For any next hop server that is configured, you can specify multiple networks by repeating this command with the same *nhs-address* argument, but with different IP network addresses.

Examples

The following example shows how to register a hub to a spoke using NBMA and FQDN:

```
Device# configure terminal
Device(config)# interface tunnel 1
Device(config-if)# ip nhrp nhs 192.0.2.1 nbma examplehub.example1.com
```

The following example shows how to configure the desired **max-connections** value:

```
Device# configure terminal
Device(config)# interface tunnel 1
Device(config-if)# ip nhrp nhs cluster 5 max-connections 100
```

The following example shows how to configure NHS priority and group values:

```
Device# configure terminal
Device(config)# interface tunnel 1
Device(config-if)# ip nhrp nhs 192.0.2.1 priority 1 cluster 2
```

Related Commands	Command	Description
	ip nhrp map	Statically configures the IP-to-NBMA address mapping of IP destinations connected to an NBMA network.
	show ip nhrp	Displays NHRP mapping information.

ipv6 nd cache expire

To configure the duration of time before an IPv6 neighbor discovery cache entry expires, use the **ipv6 nd cache expire** command in the interface configuration mode. To remove this configuration, use the **no** form of this command.

```
ipv6 nd cache expire expire-time-in-seconds [refresh]
no ipv6 nd cache expire expire-time-in-seconds [refresh]
```

Syntax Description	<i>expire-time-in-seconds</i>	The time range is from 1 through 65536 seconds. The default is 14400 seconds or 4 hours.								
	refresh	(Optional) Automatically refreshes the neighbor discovery cache entry.								
Command Modes	Interface configuration (config-if)									
Command History	<table border="1"> <thead> <tr> <th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td><td>This command was introduced.</td></tr> </tbody> </table>		Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.				
Release	Modification									
Cisco IOS XE Everest 16.6.1	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:									
	<pre>Device> enable Device# configure terminal Device(config)# interface gigabitethernet 1/1/4 Device(config-if)# ipv6 nd cache expire 7200</pre>									
Related Commands	<table border="1"> <thead> <tr> <th>Command</th><th>Description</th></tr> </thead> <tbody> <tr> <td>ipv6 nd na glean</td><td>Configures neighbor discovery to glean an entry from an unsolicited neighbor advertisement.</td></tr> <tr> <td>ipv6 nd nud retry</td><td>Configures the number of times neighbor unreachability detection resends neighbor solicitations.</td></tr> <tr> <td>show ipv6 interface</td><td>Displays the usability status of interfaces that are configured for IPv6.</td></tr> </tbody> </table>		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.
Command	Description									
ipv6 nd na glean	Configures neighbor discovery to glean an entry from an unsolicited neighbor advertisement.									
ipv6 nd nud retry	Configures the number of times neighbor unreachability detection resends neighbor solicitations.									
show ipv6 interface	Displays the usability status of interfaces that are configured for IPv6.									

ipv6 nd na glean

To configure the neighbor discovery to glean an entry from an unsolicited neighbor advertisement, use the **ipv6 nd na glean** command in the interface configuration mode. To disable this feature, use the **no** form of this command.

ipv6 nd na glean
no ipv6 nd na glean

Command Modes	Interface configuration									
Command History	Release	Modification								
	Cisco IOS XE Everest 16.6.1	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:									
	<pre>Device> enable Device# configure terminal Device(config)# interface gigabitethernet 1/1/4 Device(config-if)# ipv6 nd na glean</pre>									
Related Commands	<table border="1"> <thead> <tr> <th>Command</th><th>Description</th></tr> </thead> <tbody> <tr> <td>ipv6 nd cache expire</td><td>Configures the duration of time before an IPv6 neighbor discovery cache entry expires.</td></tr> <tr> <td>ipv6 nd nud retry</td><td>Configures the number of times neighbor unreachability detection resends neighbor solicitations.</td></tr> <tr> <td>show ipv6 interface</td><td>Displays the usability status of interfaces that are configured for IPv6.</td></tr> </tbody> </table>		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.
Command	Description									
ipv6 nd cache expire	Configures the duration of time before an IPv6 neighbor discovery cache entry expires.									
ipv6 nd nud retry	Configures the number of times neighbor unreachability detection resends neighbor solicitations.									
show ipv6 interface	Displays the usability status of interfaces that are configured for IPv6.									

ipv6 nd nud retry

To configure the number of times the neighbor unreachability detection process resends neighbor solicitations, use the **ipv6 nd nud retry** command in the interface configuration mode. To disable this feature, use the **no** form of this command.

ipv6 nd nud retry base interval max-attempts {final-wait-time}

ipv6 nd nud retry

no ipv6 nd nud retry base interval max-attempts {final-wait-time}

Syntax Description	<i>base</i>	The neighbor unreachability detection process base value.
	<i>interval</i>	The time interval, in milliseconds, between retries. The range is from 1000 to 32000.
	<i>max-attempts</i>	The maximum number of retry attempts, depending on the base value. The range is from 1 to 128.
	<i>final-wait-time</i>	The waiting time, in milliseconds, on the last probe. The range is from 1000 to 32000.
Command Modes	Interface configuration (config-if)	
Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	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:

$$tm^{\wedge}n$$

here,

- t = Time interval
 - m = Base (1, 2, or 3)
 - n = Current neighbor solicitation number (where the first neighbor solicitation is 0).

Therefore, **ipv6 nd nud retry 3 1000 5** command retransmits at intervals of 1,3,9,27,81 seconds. If the final wait time is not configured, the entry remains for 243 seconds before it is deleted.

The **ipv6 nd nud retry** command affects only the retransmit rate for the neighbor unreachability detection process, and not for the initial resolution, which uses the default of three neighbor solicitation packets sent 1 second apart.

Examples

The following example shows how to configure a fixed interval of 1 second and three retransmits:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/1/4
Device(config-if)# ipv6 nd nud retry 1 1000 3
```

The following example shows how to configure a retransmit interval of 1, 2, 4, and 8:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/1/4
Device(config-if)# ipv6 nd nud retry 2 1000 4
```

The following example shows how to configure the retransmit intervals of 1, 3, 9, 27, 81:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/1/4
Device(config-if)# ipv6 nd nud retry 3 1000 5
```

Related Commands	Command	Description
	ipv6 nd cache expire	Configures the duration of time before an IPv6 neighbor discovery (ND) cache entry expires.
	ipv6 nd na glean	Configures neighbor discovery to glean an entry from an unsolicited neighbor advertisement.
	show ipv6 interface	Displays the usability status of interfaces that are configured for IPv6.

key chain

To define an authentication key chain needed to enable authentication for routing protocols and enter key-chain configuration mode, use the **key chain** command in global configuration mode. To remove the key chain, use the **no** form of this command.

```
key chain name-of-chain
no key chain name-of-chain
```

Syntax Description	<i>name-of-chain</i>	Name of a key chain. A key chain must have at least one key and can have up to 2147483647 keys.
--------------------	----------------------	---

Command Default No key chain exists.

Command Modes Global configuration (config)

Usage Guidelines You must configure a key chain with keys to enable authentication.

Although you can identify multiple key chains, we recommend using one key chain per interface per routing protocol. Upon specifying the **key chain** command, you enter key chain configuration mode.

Examples The following example shows how to specify key chain:

```
Device (config-keychain-key) # key-string chestnut
```

key-string (authentication)

Related Commands	Command	Description
	accept-lifetime	Sets the time period during which the authentication key on a key chain is received as valid.
	key	Identifies an authentication key on a key chain.
	key-string (authentication)	Specifies the authentication string for a key.
	send-lifetime	Sets the time period during which an authentication key on a key chain is valid to be sent.
	show key chain	Displays authentication key information.

key-string (authentication)

To specify the authentication string for a key, use the **key-string(authentication)** command in key chain key configuration mode. To remove the authentication string, use the **no** form of this command.

```
key-string key-string text
no key-string text
```

Syntax Description	<i>text</i>	Authentication string that must be sent and received in the packets using the routing protocol being authenticated. The string can contain from 1 to 80 uppercase and lowercase alphanumeric characters.
---------------------------	-------------	--

Command Default No authentication string for a key exists.

Command Modes Key chain key configuration (config-keychain-key)

Examples The following example shows how to specify the authentication string for a key:

```
Device(config-keychain-key)# key-string key1
```

Related Commands	Command	Description
	accept-lifetime	Sets the time period during which the authentication key on a key chain is received as valid.
	key	Identifies an authentication key on a key chain.
	key chain	Defines an authentication key-chain needed to enable authentication for routing protocols.
	send-lifetime	Sets the time period during which an authentication key on a key chain is valid to be sent.
	show key chain	Displays authentication key information.

key

To identify an authentication key on a key chain, use the **key** command in key-chain configuration mode. To remove the key from the key chain, use the **no** form of this command.

key *key-id*
no **key** *key-id*

Syntax Description	<i>key-id</i> Identification number of an authentication key on a key chain. The range of keys is from 0 to 2147483647. The key identification numbers need not be consecutive.
---------------------------	---

Command Default No key exists on the key chain.

Command Modes Command Modes Key-chain configuration (config-keychain)

Usage Guidelines It is useful to have multiple keys on a key chain so that the software can sequence through the keys as they become invalid after time, based on the **accept-lifetime** and **send-lifetime** key chain key command settings.

Each key has its own key identifier, which is stored locally. The combination of the key identifier and the interface associated with the message uniquely identifies the authentication algorithm and Message Digest 5 (MD5) authentication key in use. Only one authentication packet is sent, regardless of the number of valid keys. The software starts looking at the lowest key identifier number and uses the first valid key.

If the last key expires, authentication will continue and an error message will be generated. To disable authentication, you must manually delete the last valid key.

To remove all keys, remove the key chain by using the **no key chain** command.

Examples

The following example shows how to specify a key to identify authentication on a key-chain:

```
Device(config-keychain)#key 1
```

Related Commands	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.
	show key chain	Displays authentication key information.

show ip nhrp nhs

To display Next Hop Resolution Protocol (NHRP) next hop server (NHS) information, use the **show ip nhrp nhs** command in user EXEC or privileged EXEC mode.

show ip nhrp nhs

show ip nhrp nhs [{interface}] [detail] [{redundancy [{cluster number} | preempted | running | waiting]}]

Syntax Description	<table border="1"> <tr> <td>interface</td><td>(Optional) Displays NHS information currently configured on the interface. See the table below for types, number ranges, and descriptions.</td></tr> <tr> <td>detail</td><td>(Optional) Displays detailed NHS information.</td></tr> <tr> <td>redundancy</td><td>(Optional) Displays information about NHS redundancy stacks.</td></tr> <tr> <td>cluster number</td><td>(Optional) Displays redundancy cluster information.</td></tr> <tr> <td>preempted</td><td>(Optional) Displays information about NHS that failed to become active and is preempted.</td></tr> <tr> <td>running</td><td>(Optional) Displays NHSs that are currently in Responding or Expecting replies states.</td></tr> <tr> <td>waiting</td><td>(Optional) Displays NHSs awaiting to be scheduled.</td></tr> </table>	interface	(Optional) Displays NHS information currently configured on the interface. See the table below for types, number ranges, and descriptions.	detail	(Optional) Displays detailed NHS information.	redundancy	(Optional) Displays information about NHS redundancy stacks.	cluster number	(Optional) Displays redundancy cluster information.	preempted	(Optional) Displays information about NHS that failed to become active and is preempted.	running	(Optional) Displays NHSs that are currently in Responding or Expecting replies states.	waiting	(Optional) Displays NHSs awaiting to be scheduled.
interface	(Optional) Displays NHS information currently configured on the interface. See the table below for types, number ranges, and descriptions.														
detail	(Optional) Displays detailed NHS information.														
redundancy	(Optional) Displays information about NHS redundancy stacks.														
cluster number	(Optional) Displays redundancy cluster information.														
preempted	(Optional) Displays information about NHS that failed to become active and is preempted.														
running	(Optional) Displays NHSs that are currently in Responding or Expecting replies states.														
waiting	(Optional) Displays NHSs awaiting to be scheduled.														

Command Modes User EXEC (>)

Privileged EXEC (#)

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

Usage Guidelines The table below lists the valid types, number ranges, and descriptions for the optional *interface* argument.



Note The valid types can vary according to the platform and interfaces on the platform.

Table 14: Valid Types, Number Ranges, and Interface Descriptions

Valid Types	Number Ranges	Interface Descriptions
ANI	0 to 1000	Autonomic-Networking virtual interface
Auto-Template	1 to 999	Auto-Template interface
GMPLS	0 to 1000	Multiprotocol Label Switching (MPLS) interface
GigabitEthernet	0 to 9	GigabitEthernet IEEE 802.3z
InternalInterface	0 to 9	Internal interface
LISP	0 to 65520	Locator/ID Separation Protocol (LISP) virtual interface
loopback	0 to 2147483647	Loopback interface
Null	0 to 0	Null interface

Valid Types	Number Ranges	Interface Descriptions
PROTECTION_GROUP	0 to 0	Protection-group controller
Port-channel	1 to 128	Port channel interface
TenGigabitEthernet	0 to 9	TenGigabitEthernet interface
Tunnel	0 to 2147483647	Tunnel interface
Tunnel-tp	0 to 65535	MPLS Transport Profile interface
Vlan	1 to 4094	VLAN interface

Examples

The following is sample output from the **show ip nhrp nhs detail** command:

```
Switch# show ip nhrp nhs detail

Legend:
  E=Expecting replies
  R=Responding
Tunnell1:
  10.1.1.1      E  req-sent 128  req-failed 1  repl-recv 0
Pending Registration Requests:
Registration Request: Reqid 1, Ret 64  NHS 10.1.1.1
```

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

Table 15: show ip nhrp nhs Field Descriptions

Field	Description
Tunnell1	Interface through which the target network is reached.

Related Commands

Command	Description
ip nhrp map	Statically configures the IP-to-NBMA address mapping of IP destinations connected to an NBMA network.
show ip nhrp	Displays NHRP mapping information.

show ip ports all

To display all the open ports on a device, use the **show ip ports all** in user EXEC or privileged EXEC mode.

show ip ports all**Syntax Description**

Syntax Description

This command has no arguments or keywords.

show ip ports all

Command Default	No default behavior or values.				
Command Modes	User EXEC (>) Privileged EXEC (#)				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				
Usage Guidelines					
<p>This command provides a list of all open TCP/IP ports on the system including the ports opened using Cisco networking stack.</p> <p>To close open ports, you can use one of the following methods:</p> <ul style="list-style-type: none"> • 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 16: Field Descriptions of show ip ports all

Field	Description
Protocol	Transport protocol used.
Local Address.	Device IP Address.
Foreign Address	Remote or peer address.
State	State of the connection. It can be listen, established or connected.
PID/Program Name	Process ID or name

Related Commands	Command	Description
	show tcp brief all	Displays information about TCP connection endpoints.
	show ip sockets	Displays IP sockets information.

show key chain

To display the keychain, use the **show key chain** command.

show key chain [name-of-chain]

Syntax Description	<i>name-of-chain</i> (Optional) Name of the key chain to display, as named in the key chain command.
---------------------------	--

Command Default If the command is used without any parameters, then it lists out all the key chains.

Command Modes Privileged EXEC (#)

Examples The following is sample output from the **show key chain** command:

```
show key chain
Device# show key chain

Key-chain AuthenticationGLBP:
    key 1 -- text "Thisisasecretkey"
        accept lifetime (always valid) - (always valid) [valid now]
        send lifetime (always valid) - (always valid) [valid now]
Key-chain glbp2:
    key 100 -- text "abc123"
        accept lifetime (always valid) - (always valid) [valid now]
        send lifetime (always valid) - (always valid) [valid now]
```

Related Commands	Command	Description
	key-string	Specifies the authentication string for a key.
	send-lifetime	Sets the time period during which an authentication key on a key chain is valid to be sent.

show track

To display information about objects that are tracked by the tracking process, use the **show track** command in privileged EXEC mode.

show track [{object-number [brief] | application [brief] | interface [brief] | ip[route [brief] | [sla [brief]] | ipv6 [route [brief]] | list [route [brief]] | resolution [ip | ipv6] | stub-object [brief] | summary | timers}]}

show track

Syntax Description	<table border="1"> <tr> <td><i>object-number</i></td><td>(Optional) Object number that represents the object to be tracked. The range is from 1 to 1000.</td></tr> <tr> <td>brief</td><td>(Optional) Displays a single line of information related to the preceding argument or keyword.</td></tr> <tr> <td>application</td><td>(Optional) Displays tracked application objects.</td></tr> <tr> <td>interface</td><td>(Optional) Displays tracked interface objects.</td></tr> <tr> <td>ip route</td><td>(Optional) Displays tracked IP route objects.</td></tr> <tr> <td>ip sla</td><td>(Optional) Displays tracked IP SLA objects.</td></tr> <tr> <td>ipv6 route</td><td>(Optional) Displays tracked IPv6 route objects.</td></tr> <tr> <td>list</td><td>(Optional) Displays the list of boolean objects.</td></tr> <tr> <td>resolution</td><td>(Optional) Displays resolution of tracked parameters.</td></tr> <tr> <td>summary</td><td>(Optional) Displays the summary of the specified object.</td></tr> <tr> <td>timers</td><td>(Optional) Displays polling interval timers.</td></tr> </table>	<i>object-number</i>	(Optional) Object number that represents the object to be tracked. The range is from 1 to 1000.	brief	(Optional) Displays a single line of information related to the preceding argument or keyword.	application	(Optional) Displays tracked application objects.	interface	(Optional) Displays tracked interface objects.	ip route	(Optional) Displays tracked IP route objects.	ip sla	(Optional) Displays tracked IP SLA objects.	ipv6 route	(Optional) Displays tracked IPv6 route objects.	list	(Optional) Displays the list of boolean objects.	resolution	(Optional) Displays resolution of tracked parameters.	summary	(Optional) Displays the summary of the specified object.	timers	(Optional) Displays polling interval timers.
<i>object-number</i>	(Optional) Object number that represents the object to be tracked. The range is from 1 to 1000.																						
brief	(Optional) Displays a single line of information related to the preceding argument or keyword.																						
application	(Optional) Displays tracked application objects.																						
interface	(Optional) Displays tracked interface objects.																						
ip route	(Optional) Displays tracked IP route objects.																						
ip sla	(Optional) Displays tracked IP SLA objects.																						
ipv6 route	(Optional) Displays tracked IPv6 route objects.																						
list	(Optional) Displays the list of boolean objects.																						
resolution	(Optional) Displays resolution of tracked parameters.																						
summary	(Optional) Displays the summary of the specified object.																						
timers	(Optional) Displays polling interval timers.																						

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

Command History	Release	Modification
		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 17: 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)

vrrp**Command History**

Release	Modification
Cisco IOS XE Everest 16.6.1	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

<i>group-id</i>	Virtual router group number. The range is from 1 to 255.
-----------------	--

address-family	Specifies the address-family for this VRRP group.
ipv4	(Optional) Specifies IPv4 address.
ipv6	(Optional) Specifies IPv6 address.

Command Default None**Command Modes** Interface configuration (config-if)

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	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 Everest 16.6.1	This command was introduced.

Examples The following example enables VRRP. VRRP group 1 is described as Building A – Marketing and Administration.

vrrp preempt

```
Device(config-if-vrrp)# description Building A - Marketing and Administration
```

Related Commands

Command	Description
vrrp	Creates a VRRPv3 group and enters VRRPv3 group configuration mode.

vrrp preempt

To configure the device to take over as master virtual router for a Virtual Router Redundancy Protocol (VRRP) group if it has higher priority than the current master virtual router, use the **preempt** command in VRRP configuration mode. To disable this function, use the **no** form of this command.

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

Syntax Description

delay minimum seconds	(Optional) Number of seconds that the device will delay before issuing an advertisement claiming master ownership. The default delay is 0 seconds.
------------------------------	--

Command Default

This command is enabled.

Command Modes

VRRP configuration (config-if-vrrp)

Command History

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines

By default, the device being configured with this command will take over as master virtual router for the group if it has a higher priority than the current master virtual router. You can configure a delay, which will cause the VRRP device to wait the specified number of seconds before issuing an advertisement claiming master ownership.



Note The device that is the IP address owner will preempt, regardless of the setting of this command.

Examples

The following example configures the device to preempt the current master virtual router when its priority of 200 is higher than that of the current master virtual router. If the device preempts the current master virtual router, it waits 15 seconds before issuing an advertisement claiming it is the master virtual router.

```
Device(config-if-vrrp)#preempt delay minimum 15
```

Related Commands	Command	Description
	vrrp	Creates a VRRPv3 group and enters VRRPv3 group configuration mode.
	priority	Sets the priority level of the device within a VRRP group.

vrrp priority

To set the priority level of the device within a Virtual Router Redundancy Protocol (VRRP) group, use the **priority** command in interface configuration mode. To remove the priority level of the device, use the **no** form of this command.

priority *level*
no priority *level*

Syntax Description	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 Everest 16.6.1	This command was introduced.

Usage Guidelines Use this command to control which device becomes the master virtual router.

Examples The following example configures the device with a priority of 254:

```
Device(config-if-vrrp)# priority 254
```

Related Commands	Command	Description
	vrrp	Creates a VRRPv3 group and enters VRRPv3 group configuration mode.
	vrrp preempt	Configures the device to take over as master virtual router for a VRRP group if it has higher priority than the current master virtual router.

vrrp timers advertise

To configure the interval between successive advertisements by the master virtual router in a Virtual Router Redundancy Protocol (VRRP) group, use the **timers advertise** command in VRRP configuration mode. To restore the default value, use the **no** form of this command.

timers advertise [*msec*] *interval*

no timers advertise [msec] interval

Syntax Description	<table border="1"> <tr> <td>group</td><td>Virtual router group number. The group number range is from 1 to 255.</td></tr> <tr> <td>msec</td><td>(Optional) Changes the unit of the advertisement time from seconds to milliseconds. Without this keyword, the advertisement interval is in seconds.</td></tr> <tr> <td>interval</td><td>Time interval between successive advertisements by the master virtual router. The unit of the interval is in seconds, unless the msec keyword is specified. The default is 1 second. The valid range is 1 to 255 seconds. When the msec keyword is specified, the valid range is 50 to 999 milliseconds.</td></tr> </table>	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 master virtual router. The unit of the interval is in seconds, unless the msec keyword is specified. The default is 1 second. The valid range is 1 to 255 seconds. When the msec keyword is specified, the valid range is 50 to 999 milliseconds.
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 master virtual router. The unit of the interval is in seconds, unless the msec keyword is specified. The default is 1 second. The valid range is 1 to 255 seconds. When the msec keyword is specified, the valid range is 50 to 999 milliseconds.						

Command Default The default interval of 1 second is configured.

Command Modes VRRP configuration (config-if-vrrp)

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines The advertisements being sent by the master virtual router communicate the state and priority of the current master virtual router.

The **vrrp timers advertise** command configures the time between successive advertisement packets and the time before other routers declare the master router to be down. Routers or access servers on which timer values are not configured can learn timer values from the master router. The timers configured on the master router always override any other timer settings. All routers in a VRRP group must use the same timer values. If the same timer values are not set, the devices in the VRRP group will not communicate with each other and any misconfigured device will change its state to master.

Examples The following example shows how to configure the master virtual router to send advertisements every 4 seconds:

```
Device(config-if-vrrp)# timers advertise 4
```

Related Commands	Command	Description
	vrrp	Creates a VRRPv3 group and enters VRRPv3 group configuration mode.
	timers learn	Configures the device, when it is acting as backup virtual router for a VRRP group, to learn the advertisement interval used by the master virtual router.

vrss leader

To specify a leader's name to be registered with Virtual Router Redundancy Service (VRRS), use the **vrss leader** command. To remove the specified VRRS leader, use the **no** form of this command.

vrrs leader *vrrs-leader-name*
no vrrs leader *vrrs-leader-name*

Syntax Description	<i>vrrs-leader-name</i>	Name of VRRS Tag to lead.
---------------------------	-------------------------	---------------------------

Command Default A registered VRRS name is unavailable by default.

Command Modes VRRP configuration (config-if-vrrp)

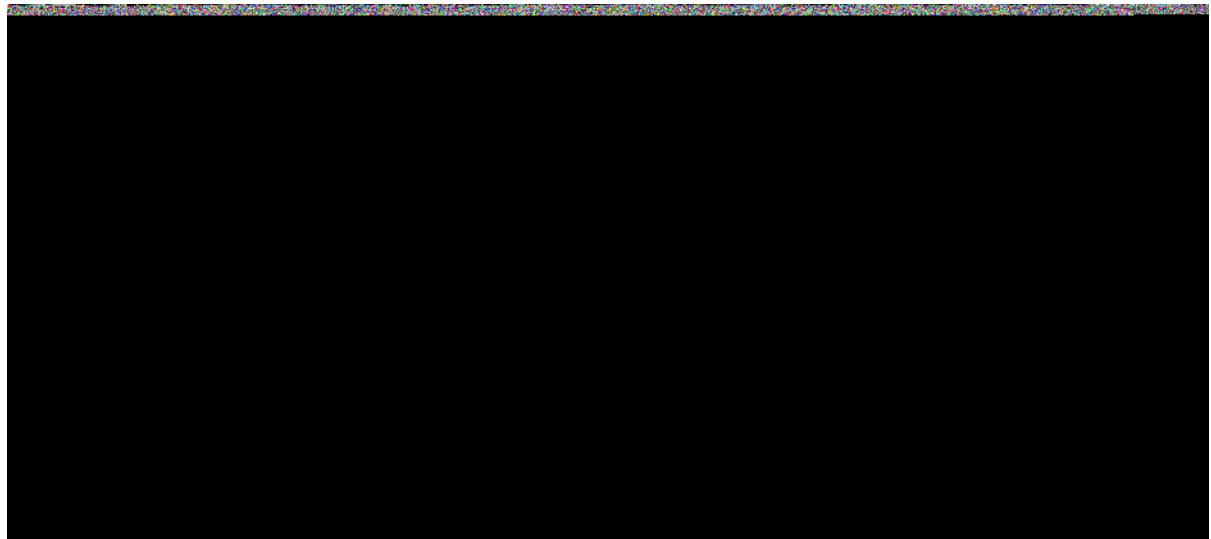
Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

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.

vrrs leader



PART **V**

IP Multicast Routing

- [IP Multicast Routing Commands, on page 217](#)

CHAPTER 0

IP Multicast Routing Commands

- [clear ip igmp snooping membership](#), on page 218
- [clear ip mfib counters](#), on page 218
- [clear ip mroute](#), on page 219
- [clear ip pim snooping vlan](#), on page 220
- [ip igmp filter](#), on page 221
- [ip igmp max-groups](#), on page 222
- [ip igmp profile](#), on page 223
- [ip igmp snooping](#), on page 224
- [ip igmp snooping last-member-query-count](#), on page 225
- [ip igmp snooping querier](#), on page 226
- [ip igmp snooping report-suppression](#), on page 228
- [ip igmp snooping vlan explicit-tracking](#), on page 229
- [ip igmp snooping vlan mrouter](#), on page 230
- [ip igmp snooping vlan static](#), on page 230
- [ip multicast auto-enable](#), on page 231
- [ip pim accept-register](#), on page 232
- [ip pim bsr-candidate](#), on page 233
- [ip pim rp-candidate](#), on page 234
- [ip pim send-rp-announce](#), on page 235
- [ip pim snooping](#), on page 236
- [ip pim snooping dr-flood](#), on page 237
- [ip pim snooping vlan](#), on page 238
- [ip pim spt-threshold](#), on page 239
- [match message-type](#), on page 239
- [match service-type](#), on page 240
- [match service-instance](#), on page 241
- [mrinfo](#), on page 241
- [service-policy-query](#), on page 242
- [service-policy](#), on page 243
- [show ip igmp filter](#), on page 244
- [show ip igmp profile](#), on page 244
- [show ip igmp snooping](#), on page 245
- [show ip igmp snooping groups](#), on page 247

clear ip igmp snooping membership

- [show ip igmp snooping membership, on page 248](#)
- [show ip igmp snooping mrouter, on page 250](#)
- [show ip igmp snooping querier, on page 250](#)
- [show ip pim autorp, on page 252](#)
- [show ip pim bsr-router, on page 253](#)
- [show ip pim bsr, on page 253](#)
- [show ip pim snooping, on page 254](#)
- [show ip pim tunnel, on page 257](#)
- [show platform software fed switch ip multicast, on page 258](#)

clear ip igmp snooping membership

To remove entries from the explicit host-tracking database, use the **clear ip igmp snooping membership** command in the privileged EXEC mode.

clear ip igmp snooping membership [vlan *vlan-id*]

Syntax Description	vlan <i>vlan-id</i> (Optional) Specifies a VLAN; valid values are from 1 to 1001 and from 1006 to 4094.						
Command Default	This command has no default settings.						
Command Modes	Privileged EXEC (#)						
	<table border="1"> <thead> <tr> <th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td>Cisco IOS XE Fuji 16.8.1a</td><td>This command was introduced.</td></tr> </tbody> </table>	Release	Modification	Cisco IOS XE Fuji 16.8.1a	This command was introduced.		
Release	Modification						
Cisco IOS XE Fuji 16.8.1a	This command was introduced.						
Usage Guidelines	Entries in the IGMP Snooping Membership table do not age out or get cleared on their own. Use the clear ip igmp snooping membership command to remove the old or stale entries from the table.						
Example	<pre>Device# clear ip igmp snooping membership vlan 25 Device#</pre>						
Related Commands	<table border="1"> <thead> <tr> <th>Command</th><th>Description</th></tr> </thead> <tbody> <tr> <td>ip igmp snooping vlan explicit-tracking</td><td>Enables per-VLAN explicit host tracking.</td></tr> <tr> <td>show ip igmp snooping membership</td><td>Displays host membership information.</td></tr> </tbody> </table>	Command	Description	ip igmp snooping vlan explicit-tracking	Enables per-VLAN explicit host tracking.	show ip igmp snooping membership	Displays host membership information.
Command	Description						
ip igmp snooping vlan explicit-tracking	Enables per-VLAN explicit host tracking.						
show ip igmp snooping membership	Displays host membership information.						

clear ip mfib counters

To clear all the active IPv4 Multicast Forwarding Information Base (MFIB) traffic counters, use the **clear ip mfib counters** command in privileged EXEC mode.

clear ip mfib [global | vrf *] counters [group-address] [hostname | source-address]

Syntax Description	global (Optional) Resets the IP MFIB cache to the global default configuration. vrf * (Optional) Clears the IP MFIB cache for all VPN routing and forwarding instances. <i>group-address</i> (Optional) Limits the active MFIB traffic counters to the indicated group address. <i>hostname</i> (Optional) Limits the active MFIB traffic counters to the indicated host name. <i>source-address</i> (Optional) Limits the active MFIB traffic counters to the indicated source address.
Command Default	None
Command Modes	Privileged EXEC (#)
Command History	Release Modification Cisco IOS XE Everest 16.6.1 This command was introduced.

Example

The following example shows how to reset all the active MFIB traffic counters for all the multicast tables:

```
Device# clear ip mfib counters
```

The following example shows how to reset the IP MFIB cache counters to the global default configuration:

```
Device# clear ip mfib global counters
```

The following example shows how to clear the IP MFIB cache for all the VPN routing and forwarding instances:

```
Device# clear ip mfib vrf * counters
```

clear ip mroute

To delete the entries in the IP multicast routing table, use the **clear ip mroute** command in privileged EXEC mode.

clear ip mroute [vrf vrf-name] {* | ip-address | group-address} [hostname | source-address]

Syntax Description	vrf 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.
---------------------------	--

clear ip pim snooping vlan

<i>hostname</i>	(Optional) Multicast routes for the host name.
<i>source-address</i>	(Optional) Multicast routes for the source address.

Command Default None**Command Modes** Privileged EXEC**Command History** **Release** **Modification**

Cisco IOS XE Everest 16.6.1 This command was introduced.

Usage Guidelines The *group-address* variable specifies one of the following:

- Name of the multicast group as defined in the DNS hosts table or with the **ip host** command.
- IP address of the multicast group in four-part, dotted notation.

If you specify a group name or address, you can also enter the source argument to specify a name or address of a multicast source that is sending to the group. A source does not need to be a member of the group.

Example

The following example shows how to delete all the entries from the IP multicast routing table:

```
Device# clear ip mroute *
```

The following example shows how to delete all the sources on the 228.3.0.0 subnet that are sending to the multicast group 224.2.205.42 from the IP multicast routing table. This example shows how to delete all sources on network 228.3, not individual sources:

```
Device# clear ip mroute 224.2.205.42 228.3.0.0
```

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 Everest 16.6.1	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 device stack or on a standalone device. To remove the specified profile from the interface, use the **no** form of this command.

ip igmp filter *profile number*
no ip igmp filter

Syntax Description	<i>profile number</i> IGMP profile number to be applied. The range is 1—4294967295.
---------------------------	---

Command Default	No IGMP filters are applied.
------------------------	------------------------------

Command Modes	Interface configuration (config-if)
----------------------	-------------------------------------

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines	You can apply IGMP filters only to Layer 2 physical interfaces; you cannot apply IGMP filters to routed ports, switch virtual interfaces (SVIs), or ports that belong to an EtherChannel group.
-------------------------	---

An IGMP profile can be applied to one or more device port interfaces, but one port can have only one profile applied to it.

ip igmp max-groups**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 device stack or on a standalone device. To set the maximum back to the default, which is to have no maximum limit, or to return to the default throttling action, which is to drop the report, use the **no** form of this command.

```
ip igmp max-groups {max number | action { deny | replace }}
no ip igmp max-groups {max number | action}
```

Syntax Description	<p>max number Maximum number of IGMP groups that an interface can join. The range is 0—4294967294. The default is no limit.</p> <p>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.</p> <p>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.</p>
---------------------------	---

Command Default The default maximum number of groups is no limit.

After the device learns the maximum number of IGMP group entries on an interface, the default throttling action is to drop the next IGMP report that the interface receives and to not add an entry for the IGMP group to the interface.

Command Modes Interface configuration

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines You can use this command only on Layer 2 physical interfaces and on logical EtherChannel interfaces. You cannot set IGMP maximum groups for routed ports, switch virtual interfaces (SVIs), or ports that belong to an EtherChannel group.

Follow these guidelines when configuring the IGMP throttling action:

- If you configure the throttling action as deny, and set the maximum group limit, the entries that were previously in the forwarding table are not removed, but are aged out. After these entries are aged out, when the maximum number of entries is in the forwarding table, the device drops the next IGMP report received on the interface.

- If you configure the throttling action as replace, and set the maximum group limitation, the entries that were previously in the forwarding table are removed. When the maximum number of entries is in the forwarding table, the device replaces a randomly selected multicast entry with the received IGMP report.
- When the maximum group limitation is set to the default (no maximum), entering the **ip igmp max-groups {deny | replace}** command has no effect.

Example

The following example shows how to limit the number of IGMP groups that a port can join to 25:

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# ip igmp max-groups 25
```

The following example shows how to configure the device to replace the existing group with the new group for which the IGMP report was received when the maximum number of entries is in the forwarding table:

```
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# ip igmp max-groups action replace
```

You can verify your setting by using the **show running-config** privileged EXEC command and by specifying an interface.

ip igmp profile

To create an Internet Group Management Protocol (IGMP) profile and enter IGMP profile configuration mode, use the **ip igmp profile** global configuration command on the device stack or on a standalone device. From this mode, you can specify the configuration of the IGMP profile to be used for filtering IGMP membership reports from a switch port. To delete the IGMP profile, use the **no** form of this command.

ip igmp profile *profile number*
no ip igmp profile *profile number*

Syntax Description

profile number The IGMP profile number being configured. The range is from 1—4294967295.

Command Default

No IGMP profiles are defined. When configured, the default action for matching an IGMP profile is to deny matching addresses.

Command Modes

Global configuration

Command History

Release	Modification
---------	--------------

Cisco IOS XE Everest 16.6.1

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.

ip igmp snooping

- **no**—Negates a command or resets to its defaults.
- **permit**—Specifies that matching addresses are permitted.
- **range**—Specifies a range of IP addresses for the profile. This can be a single IP address or a range with a start and an end address.

When entering a range, enter the low IP multicast address, a space, and the high IP multicast address.

You can apply an IGMP profile to one or more Layer 2 interfaces, but each interface can have only one profile applied to it.

Example

The following example shows how to configure IGMP profile 40, which permits the specified range of IP multicast addresses:

```
Device(config)# ip igmp profile 40
Device(config-igmp-profile)# permit
Device(config-igmp-profile)# range 233.1.1.1 233.255.255.255
```

You can verify your settings by using the **show ip igmp profile** command in privileged EXEC mode.

ip igmp snooping

To globally enable Internet Group Management Protocol (IGMP) snooping on the device or to enable it on a per-VLAN basis, use the **ip igmp snooping** global configuration command on the device stack or on a standalone device. To return to the default setting, use the **no** form of this command.

ip igmp snooping [vlan <i>vlan-id</i>]
no ip igmp snooping [vlan <i>vlan-id</i>]

Syntax Description	vlan <i>vlan-id</i> (Optional) Enables IGMP snooping on the specified VLAN. Ranges are 1—1001 and 1006—4094.	
Command Default	IGMP snooping is globally enabled on the device. IGMP snooping is enabled on VLAN interfaces.	
Command Modes	Global configuration	
Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.
Usage Guidelines	When IGMP snooping is enabled globally, it is enabled in all of the existing VLAN interfaces. When IGMP snooping is globally disabled, it is disabled on all of the existing VLAN interfaces. VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs, and cannot be used in IGMP snooping.	

Example

The following example shows how to globally enable IGMP snooping:

```
Device(config)# ip igmp snooping
```

The following example shows how to enable IGMP snooping on VLAN 1:

```
Device(config)# ip igmp snooping vlan 1
```

You can verify your settings by entering the **show ip igmp snooping** command in privileged EXEC mode.

ip igmp snooping last-member-query-count

To configure how often Internet Group Management Protocol (IGMP) snooping will send query messages in response to receiving an IGMP leave message, use the **ip igmp snooping last-member-query-count** command in global configuration mode. To set *count* to the default value, use the **no** form of this command.

```
ip igmp snooping [vlan vlan-id] last-member-query-count count  
no ip igmp snooping [vlan vlan-id] last-member-query-count count
```

Syntax Description	vlan <i>vlan-id</i> (Optional) Sets the count value on a specific VLAN ID. The range is from 1—1001. Do not enter leading zeroes. count Interval at which query messages are sent, in milliseconds. The range is from 1—7. The default is 2.				
Command Default	A query is sent every 2 milliseconds.				
Command Modes	Global configuration				
Command History	<table border="1"> <thead> <tr> <th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td><td>This command was introduced.</td></tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				

Usage Guidelines When a multicast host leaves a group, the host sends an IGMP leave message. To check if this host is the last to leave the group, IGMP query messages are sent when the leave message is seen until the **last-member-query-interval** timeout period expires. If no response is received to the last-member queries before the timeout period expires, the group record is deleted.

Use the **ip igmp snooping last-member-query-interval** command to configure the timeout period.

When both IGMP snooping immediate-leave processing and the query count are configured, immediate-leave processing takes precedence.



Note Do not set the count to 1 because the loss of a single packet (the query packet from the device to the host or the report packet from the host to the device) may result in traffic forwarding being stopped even if the receiver is still there. Traffic continues to be forwarded after the next general query is sent by the device, but the interval during which a receiver may not receive the query could be as long as 1 minute (with the default query interval).

The leave latency in Cisco IOS software may increase by up to 1 last-member query interval (LMQI) value when the device is processing more than one leave within an LMQI. In such a scenario, the average leave latency is determined by the $(\text{count} + 0.5) * \text{LMQI}$. The result is that the default leave latency can range from 2.0 to 3.0 seconds with an average of 2.5 seconds under a higher load of IGMP leave processing. The leave latency under load for the minimum LMQI value of 100 milliseconds and a count of 1 is from 100 to 200 milliseconds, with an average of 150 milliseconds. This is done to limit the impact of higher rates of IGMP leave messages.

Example

The following example shows how to set the last member query count to 5:

```
Device(config)# ip igmp snooping last-member-query-count 5
```

ip igmp snooping querier

To globally enable the Internet Group Management Protocol (IGMP) querier function in Layer 2 networks, use the **ip igmp snooping querier** global configuration command. Use the command with keywords to enable and configure the IGMP querier feature on a VLAN interface. To return to the default settings, use the **no** form of this command.

```
ip igmp snooping [vlan vlan-id] querier [address ip-address | max-response-time response-time | query-interval interval-count | tcn query {count count | interval interval} | timer expiry expiry-time | version version]
no ip igmp snooping [vlan vlan-id] querier [address | max-response-time | query-interval | tcn query {count | interval} | timer expiry | version]
```

Syntax Description

vlan <i>vlan-id</i>	(Optional) Enables IGMP snooping and the IGMP querier function on the specified VLAN. Ranges are 1—1001 and 1006—4094.
address <i>ip-address</i>	(Optional) Specifies a source IP address. If you do not specify an IP address, the querier tries to use the global IP address configured for the IGMP querier.
max-response-time <i>response-time</i>	(Optional) Sets the maximum time to wait for an IGMP querier report. The range is 1—25 seconds.
query-interval <i>interval-count</i>	(Optional) Sets the interval between IGMP queriers. The range is 1—18000 seconds.

tcn query	(Optional) Sets parameters related to Topology Change Notifications (TCNs).
count count	Sets the number of TCN queries to be executed during the TCN interval time. The range is 1—10.
interval interval	Sets the TCN query interval time. The range is 1—255.
timer expiry expiry-time	(Optional) Sets the length of time until the IGMP querier expires. The range is 60—300 seconds.
version version	(Optional) Selects the IGMP version number that the querier feature uses. Select either 1 or 2.

Command Default

The IGMP snooping querier feature is globally disabled on the device.

When enabled, the IGMP snooping querier disables itself if it detects IGMP traffic from a multicast router.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines

Use this command to enable IGMP snooping to detect the IGMP version and IP address of a device that sends IGMP query messages, which is also called a querier.

By default, the IGMP snooping querier is configured to detect devices that use IGMP Version 2 (IGMPv2), but does not detect clients that are using IGMP Version 1 (IGMPv1). You can manually configure the **max-response-time** value when devices use IGMPv2. You cannot configure the max-response-time when devices use IGMPv1. (The value cannot be configured, and is set to zero).

Non-RFC-compliant devices running IGMPv1 might reject IGMP general query messages that have a non-zero value as the **max-response-time** value. If you want the devices to accept the IGMP general query messages, configure the IGMP snooping querier to run IGMPv1.

VLAN IDs 1002—1005 are reserved for Token Ring and FDDI VLANs, and cannot be used in IGMP snooping.

Example

The following example shows how to globally enable the IGMP snooping querier feature:

```
Device(config)# ip igmp snooping querier
```

The following example shows how to set the IGMP snooping querier maximum response time to 25 seconds:

```
Device(config)# ip igmp snooping querier max-response-time 25
```

The following example shows how to set the IGMP snooping querier interval time to 60 seconds:

```
Device(config)# ip igmp snooping querier query-interval 60
```

The following example shows how to set the IGMP snooping querier TCN query count to 25:

```
Device(config)# ip igmp snooping querier tcn count 25
```

ip igmp snooping report-suppression

The following example shows how to set the IGMP snooping querier timeout value to 60 seconds:

```
Device(config)# ip igmp snooping querier timer expiry 60
```

The following example shows how to set the IGMP snooping querier feature to Version 2:

```
Device(config)# ip igmp snooping querier version 2
```

You can verify your settings by entering the **show ip igmp snooping** privileged EXEC command.

ip igmp snooping report-suppression

To enable Internet Group Management Protocol (IGMP) report suppression, use the **ip igmp snooping report-suppression** global configuration command on the device stack or on a standalone device. To disable IGMP report suppression, and to forward all IGMP reports to multicast routers, use the **no** form of this command.

```
ip igmp snooping report-suppression
no ip igmp snooping report-suppression
```

Syntax Description This command has no arguments or keywords.

Command Default IGMP report suppression is enabled.

Command Modes Global configuration

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines IGMP report suppression is supported only when the multicast query has IGMPv1 and IGMPv2 reports. This feature is not supported when the query includes IGMPv3 reports.

The device uses IGMP report suppression to forward only one IGMP report per multicast router query to multicast devices. When IGMP report suppression is enabled (the default), the device sends the first IGMP report from all the hosts for a group to all the multicast routers. The device does not send the remaining IGMP reports for the group to the multicast routers. This feature prevents duplicate reports from being sent to the multicast devices.

If the multicast router query includes requests only for IGMPv1 and IGMPv2 reports, the device forwards only the first IGMPv1 or IGMPv2 report from all the hosts for a group to all of the multicast routers. If the multicast router query also includes requests for IGMPv3 reports, the device forwards all IGMPv1, IGMPv2, and IGMPv3 reports for a group to the multicast devices.

If you disable IGMP report suppression by entering the **no ip igmp snooping report-suppression** command, all IGMP reports are forwarded to all of the multicast routers.

Example

The following example shows how to disable report suppression:

```
Device(config)# no ip igmp snooping report-suppression
```

You can verify your settings by entering the **show ip igmp snooping** command in privileged EXEC mode.

ip igmp snooping vlan explicit-tracking

To enable a per-VLAN explicit tracking of hosts, groups, and channels for Internet Group Management Protocol (IGMP), use the **ip igmp snooping vlan explicit-tracking** command in global configuration mode. To disable IGMP explicit tracking, use the no form of this command.

ip igmp snooping vlan *vlan-id* explicit-tracking
no ip igmp snooping vlan *vlan-id* explicit-tracking

Syntax Description	<i>vlan-id</i>	VLAN ID; the range is 1 to 1001 and 1006 to 4094.				
Command Default	Explicit host tracking is enabled.					
Command Modes	Global configuration (config)					
<table border="1"> <thead> <tr> <th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td>Cisco IOS XE Fuji 16.8.1a</td><td>This command was introduced.</td></tr> </tbody> </table>			Release	Modification	Cisco IOS XE Fuji 16.8.1a	This command was introduced.
Release	Modification					
Cisco IOS XE Fuji 16.8.1a	This command was introduced.					
Usage Guidelines	Use the ip igmp snooping vlan explicit-tracking command to enable a multicast device to explicitly track the membership of multicast hosts in a particular multiaccess network. This capability enables the device to track each individual host that is joined to a particular group or channel and to achieve minimal leave latencies when hosts leave a multicast group or channel.					

Example

The following example shows how to enable explicit tracking.

```
Device# configure terminal
Device(config)#ip igmp snooping vlan 100 explicit-tracking
Device(config)#exit
```

The following example shows how to disable IGMP explicit host tracking on interface VLAN 200 and how to verify the configuration:

```
Device(config)# no ip igmp snooping vlan 200 explicit-tracking
Device(config)# end
Device# show ip igmp snooping vlan 200 | include explicit tracking
Global IGMP Snooping configuration:
-----
IGMP snooping : Enabled
IGMPv3 snooping : Enabled
Report suppression : Enabled
TCN solicit query : Disabled
TCN flood query count : 2

Vlan 2:
-----
IGMP snooping : Enabled
```

ip igmp snooping vlan mrouter

```

IGMPv2 immediate leave : Disabled
Explicit host tracking : Disabled
Multicast router learning mode : pim-dvmrp
CGMP interoperability mode : IGMP_ONLY
Explicit host tracking : Disabled
Device#

```

ip igmp snooping vlan mrouter

To add a multicast router port, use the **ip igmp snooping mrouter** global configuration command on the device stack or on a standalone device. To return to the default settings, use the **no** form of this command.

Command Default	By default, there are no multicast router ports.	
Command Modes	Global configuration	
Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines	VLAN IDs 1002—1005 are reserved for Token Ring and FDDI VLANs, and cannot be used in IGMP snooping. The configuration is saved in NVRAM.
-------------------------	--

Example

The following example shows how to configure a port as a multicast router port:

```
Device(config)# ip igmp snooping vlan 1 mrouter interface gigabitethernet1/0/2
```

You can verify your settings by entering the **show ip igmp snooping** privileged EXEC command.

ip igmp snooping vlan static

To enable Internet Group Management Protocol (IGMP) snooping and to statically add a Layer 2 port as a member of a multicast group, use the **ip igmp snooping vlan static** global configuration command on the device stack or on a standalone device. To remove the port specified as members of a static multicast group, use the **no** form of this command.

```

ip igmp snooping vlan vlan-id static ip-address interface interface-id
no ip igmp snooping vlan vlan-id static ip-address interface interface-id

```

Syntax Description	<i>vlan-id</i>	Enables IGMP snooping on the specified VLAN. Ranges are 1—1001 and 1006—4094.
	<i>ip-address</i>	Adds a Layer 2 port as a member of a multicast group with the specified group IP address.

interface 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 Everest 16.6.1	This command was introduced.

Usage Guidelines VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs, and cannot be used in IGMP snooping.

The configuration is saved in NVRAM.

Example

The following example shows how to statically configure a host on an interface:

```
Device(config)# ip igmp snooping vlan 1 static 224.2.4.12 interface
gigabitEthernet1/0/1
```

Configuring port gigabitethernet1/0/1 on group 224.2.4.12

You can verify your settings by entering the **show ip igmp snooping** command in privileged EXEC mode.

ip multicast auto-enable

To support authentication, authorization, and accounting (AAA) enabling of IP multicast, use the **ip multicast auto-enable** command. This command allows multicast routing to be enabled dynamically on dialup interfaces using AAA attributes from a RADIUS server. To disable IP multicast for AAA, use the **no** form of this command.

```
ip multicast auto-enable
no ip multicast auto-enable
```

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Global configuration

ip pim accept-register

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Example

The following example shows how to enable AAA on IP multicast:

```
Device(config)# ip multicast auto-enable
```

ip pim accept-register

To configure a candidate rendezvous point (RP) switch to filter Protocol Independent Multicast (PIM) register messages, use the **ip pim accept-register** command in global configuration mode. To disable this function, use the **no** form of this command.

```
ip pim [vrf vrf-name] accept-register {list access-list}
no ip pim [vrf vrf-name] accept-register
```

Syntax Description	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 <i>vrf-name</i> argument. list access-list Specifies the <i>access-list</i> argument as a number or name that defines the (S, G) traffic in PIM register messages to be permitted or denied. The range is 100—199 and the expanded range is 2000—2699. An IP-named access list can also be used.
---------------------------	---

Command Default	No PIM register filters are configured.
------------------------	---

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

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines	Use this command to prevent unauthorized sources from registering with the RP. If an unauthorized source sends a register message to the RP, the RP will immediately send back a register-stop message.
-------------------------	---

The access list provided for the **ip pim accept-register** command should only filter IP source addresses and IP destination addresses. Filtering on other fields (for example, IP protocol or UDP port number) will not be effective and may cause undesired traffic to be forwarded from the RP down the shared tree to multicast group members. If more complex filtering is required, use the **ip multicast boundary** command instead.

Example

The following example shows how to permit register packets for a source address sending to any group range, with the exception of source address 172.16.10.1 sending to the SSM group range

(232.0.0.0/8). These are denied. These statements should be configured on all candidate RPs because candidate RPs will receive PIM registers from first-hop routers or switches.

```
Device(config)# ip pim accept-register list ssm-range
Device(config)# ip access-list extended ssm-range
Device(config-ext-nacl)# deny ip any 232.0.0.0 0.255.255.255
Device(config-ext-nacl)# permit ip any any
```

ip pim bsr-candidate

To configure the Device to be a candidate BSR, use the **ip pim bsr-candidate** command in global configuration mode. To remove the switch as a candidate BSR, use the **no** form of this command.

```
ip pim [vrf vrf-name] bsr-candidate interface-id [hash-mask-length] [priority]
no ip pim [vrf vrf-name] bsr-candidate
```

Syntax Description	<p>vrf vrf-name (Optional) Configures the Device to be a candidate BSR for the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the <i>vrf-name</i> argument.</p> <p>interface-id ID of the interface on the Device from which the BSR address is derived to make it a candidate. This interface must be enabled for Protocol Independent Multicast (PIM) using the ip pim command. Valid interfaces include physical ports, port channels, and VLANs.</p> <p>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.</p> <p>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.</p>
---------------------------	---

Command Default The Device is not configured to announce itself as a candidate BSR.

Command Modes Global configuration

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines The interface specified for this command must be enabled for Protocol Independent Multicast (PIM) using the **ip pim** command.

This command configures the Device to send BSR messages to all of its PIM neighbors, with the address of the designated interface as the BSR address.

This command should be configured on backbone Devices that have good connectivity to all parts of the PIM domain.

ip pim rp-candidate

The BSR mechanism is specified in RFC 2362. Candidate RP (C-RP) switches unicast C-RP advertisement packets to the BSR. The BSR then aggregates these advertisements in BSR messages, which it regularly multicasts with a TTL of 1 to the ALL-PIM-ROUTERS group address, 224.0.0.13. The multicasting of these messages is handled by hop-by-hop RPF flooding; so, no pre-existing IP multicast routing setup is required (unlike with AutoRP). In addition, the BSR does not preselect the designated RP for a particular group range (unlike AutoRP); instead, each switch that receives BSR messages will elect RPs for group ranges based on the information in the BSR messages.

Cisco Device always accept and process BSR messages. There is no command to disable this function.

Cisco Device perform the following steps to determine which C-RP is used for a group:

- A long match lookup is performed on the group prefix that is announced by the BSR C-RPs.
- If more than one BSR-learned C-RP is found by the longest match lookup, the C-RP with the lowest priority (configured with the **ip pim rp-candidate** command) is preferred.
- If more than one BSR-learned C-RP has the same priority, the BSR hash function is used to select the RP for a group.
- If more than one BSR-learned C-RP returns the same hash value derived from the BSR hash function, the BSR C-RP with the highest IP address is preferred.

Example

The following example shows how to configure the IP address of theDevice on Gigabit Ethernet interface 1/0/0 to be a BSR C-RP with a hash mask length of 0 and a priority of 192:

```
Device(config)# ip pim bsr-candidate GigabitEthernet1/0/1 0 192
```

ip pim rp-candidate

To configure the Device to advertise itself to the BSR as a Protocol Independent Multicast (PIM) Version 2 (PIMv2) candidate rendezvous point (C-RP), use the **ip pim rp-candidate** command in global configuration mode. To remove the Device as a C-RP, use the **no** form of this command.

```
ip pim [vrf vrf-name] rp-candidate interface-id [group-list access-list-number]
no ip pim [vrf vrf-name] rp-candidate interface-id [group-list access-list-number]
```

Syntax Description	vrf 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 <i>vrf-name</i> 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 (Optional) Specifies the standard IP access list number that defines the group prefixes that are advertised in association with the RP address.

Command Default The Device is not configured to announce itself to the BSR as a PIMv2 C-RP.

Command Modes	Global configuration	
Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.
Usage Guidelines	<p>Use this command to configure the Device to send PIMv2 messages so that it advertises itself as a candidate RP to the BSR.</p> <p>This command should be configured on backbone Devices that have good connectivity to all parts of the PIM domain.</p> <p>The IP address associated with the interface specified by <i>interface-id</i> will be advertised as the C-RP address.</p> <p>The interface specified for this command must be enabled for Protocol Independent Multicast (PIM) using the ip pim command.</p> <p>If the optional group-list keyword and <i>access-list-number</i> argument are configured, the group prefixes defined by the standard IP access list will also be advertised in association with the RP address.</p>	
Example		

The following example shows how to configure the switch to advertise itself as a C-RP to the BSR in its PIM domain. The standard access list number 4 specifies the group prefix associated with the RP that has the address identified by Gigabit Ethernet interface 1/0/1.

```
Device(config)# ip pim rp-candidate GigabitEthernet1/0/1 group-list 4
```

ip pim send-rp-announce

To use Auto-RP to configure groups for which the Device will act as a rendezvous point (RP), use the **ip pim send-rp-announce** command in global configuration mode. To unconfigure the Device as an RP, use the **no** form of this command.

```
ip pim [vrf vrf-name] send-rp-announce interface-id scope ttl-value [group-list access-list-number]
[interval seconds]
no ip pim [vrf vrf-name] send-rp-announce interface-id
```

Syntax Description	vrf vrf-name	(Optional) Uses Auto-RP to configure groups for which the Device will act as a rendezvous point (RP) for the <i>vrf-name</i> argument.
	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.

ip pim snooping

group-list <i>access-list-number</i>	(Optional) Specifies the standard IP access list number that defines the group prefixes that are advertised in association with the RP address. Enter an IP standard access list number from 1—99. If no access list is configured, the RP is used for all groups.				
interval <i>seconds</i>	(Optional) Specifies the interval between RP announcements, in seconds. The total hold time of the RP announcements is automatically set to three times the value of the interval. The default interval is 60 seconds. The range is 1—16383.				
Command Default	Auto-RP is disabled.				
Command Modes	Global configuration				
Command History	<table border="1"> <thead> <tr> <th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td><td>This command was introduced.</td></tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				

Usage Guidelines	Enter this command on the Device that you want to be an RP. When you are using Auto-RP to distribute group-to-RP mappings, this command causes the router to send an Auto-RP announcement message to the well-known group CISCO-RP-ANNOUNCE (224.0.1.39). This message announces the router as a candidate RP for the groups in the range described by the access list.
-------------------------	---

Example

The following example shows how to configure the Device to send RP announcements out all Protocol Independent Multicast (PIM)-enabled interfaces for a maximum of 31 hops. The IP address by which the switch wants to be identified as RP is the IP address associated with Gigabit Ethernet interface 1/0/1 at an interval of 120 seconds:

```
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 Everest 16.6.1	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 Everest 16.6.1	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.

ip pim snooping vlan**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

<i>vlan-id</i>	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 Everest 16.6.1	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	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				

Example

The following example shows how to make all the sources for access list 16 use the shared tree:

```
Device(config)# ip pim spt-threshold infinity group-list 16
```

match message-type

To set a message type to match a service list, use the **match message-type** command.

```
match message-type {announcement | any | query}
```

match service-type

Syntax Description	announcement Allows only service advertisements or announcements for the Device. any Allows any match type. query Allows only a query from the client for a certain Device in the network.				
Command Default	None				
Command Modes	Service list configuration.				
Command History	<table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; width: 30%;">Release</th> <th style="text-align: left;">Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	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	 <p>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.</p>				

Example

The following example shows how to set the announcement message type to be matched:

```
Device(config-mdns-sd-sl)# match message-type announcement
```

match service-type

To set the value of the mDNS service type string to match, use the **match service-type** command.

match service-type line

Syntax Description	<i>line</i> Regular expression to match the service type in packets.				
Command Default	None				
Command Modes	Service list configuration				
Command History	<table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; width: 30%;">Release</th> <th style="text-align: left;">Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				

Usage Guidelines

It is not possible to use the **match** command if you have used the **service-list mdns-sd *service-list-name* query** command. The **match** command can be used only for the **permit** or **deny** option.

Example

The following example shows how to set the value of the mDNS service type string to match:

```
Device(config-mdns-sd-s1)# 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
Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines

It is not possible to use the **match** command if you have used the **service-list mdns-sd *service-list-name* query** command. The **match** command can be used only for the **permit** or **deny** option.

Example

The following example shows how to set the service instance to match:

```
Device(config-mdns-sd-s1)# 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.

service-policy-query

Command Default	The command is disabled.				
Command Modes	User EXEC Privileged EXEC				
Command History	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; padding-bottom: 5px;">Release</th><th style="text-align: left; padding-bottom: 5px;">Modification</th></tr> </thead> <tbody> <tr> <td style="padding-top: 5px;">Cisco IOS XE Everest 16.6.1</td><td style="padding-top: 5px;">This command was introduced.</td></tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				

Usage Guidelines The **mrinfo** command is the original tool of the multicast backbone (MBONE) to determine which neighboring multicast routers or switches are peering with multicast routers or switches. Cisco routers supports **mrinfo** requests from Cisco IOS Release 10.2.

You can query a multicast router or multilayer switch using the **mrinfo** command. The output format is identical to the multicast routed version of the Distance Vector Multicast Routing Protocol (DVMRP). (The mrouted software is the UNIX software that implements DVMRP.)

Example

The following is the sample output from the **mrinfo** command:

```
Device# mrinfo
vrf 192.0.1.0
192.31.7.37 (barnet-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 Everest 16.6.1	This command was introduced.

Usage Guidelines Since there are devices that do not send unsolicited announcements and to force such devices the learning of services and to keep them refreshed in the cache, this command contains an active query feature that ensures that the services listed in the active query list are queried.

Example

This example shows how to configure service list query periodicity:

```
Device(config-mdns)# service-policy-query sl-query1 100
```

service-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 Everest 16.6.1	This command was introduced.

Example

The following example shows how to apply a filter on incoming service-discovery information on a service list:

```
Device(config-mdns)# service-policy serv-pol1 IN
```

show ip igmp filter

show ip igmp filter

To display Internet Group Management Protocol (IGMP) filter information, use the **show ip igmp filter** command in privileged EXEC mode.

show ip igmp [vrf *vrf-name*] filter

Syntax Description	<i>vrf vrf-name</i> (Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
---------------------------	--

Command Default	IGMP filters are enabled by default.
------------------------	--------------------------------------

Command Modes	Privileged EXEC
----------------------	-----------------

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines	The show ip igmp filter command displays information about all filters defined on the device.
-------------------------	--

Example

The following example shows the sample output from the **show ip igmp filter** command:

```
Device# show ip igmp filter
IGMP filter enabled
```

show ip igmp profile

To display all the configured Internet Group Management Protocol (IGMP) profiles or a specified IGMP profile, use the **show ip igmp profile** command in privileged EXEC mode.

show ip igmp [vrf *vrf-name*] profile [*profile number*]

Syntax Description	<i>vrf vrf-name</i> (Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
---------------------------	--

<i>profile number</i>	(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 Everest 16.6.1	This command was introduced.
-----------------------------	------------------------------

Usage Guidelines	None
-------------------------	------

Examples

The following example shows the output of the **show ip igmp profile** command for profile number 40 on the device:

```
Device# show ip igmp profile 40
IGMP Profile 40
  permit
    range 233.1.1.1 233.255.255.255
```

The following example shows the output of the **show ip igmp profile** command for all the profiles configured on the device:

```
Device# show ip igmp profile

IGMP Profile 3
  range 230.9.9.0 230.9.9.0
IGMP Profile 4
  permit
    range 229.9.9.0 229.255.255.255
```

show ip igmp snooping

To display the Internet Group Management Protocol (IGMP) snooping configuration of the device or the VLAN, use the **show ip igmp snooping** command in user EXEC or privileged EXEC mode.

show ip igmp snooping [groups | mrouter | querier] [vlan vlan-id] [detail]

Syntax Description	groups (Optional) Displays the IGMP snooping multicast table. mrouter (Optional) Displays the IGMP snooping multicast router ports. querier (Optional) Displays the configuration and operation information for the IGMP querier. vlan vlan-id (Optional) Specifies a VLAN; the range is 1 to 1001 and 1006 to 4094. detail (Optional) Displays operational state information.				
Command Default	None				
Command Modes	User EXEC Privileged EXEC				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	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.				

show ip igmp snooping

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

Examples

The following is a sample output from the **show ip igmp snooping vlan 1** command. It shows snooping characteristics for a specific VLAN:

```
Device# show ip igmp snooping vlan 1

Global IGMP Snooping configuration:
-----
IGMP snooping : Enabled
IGMPv3 snooping (minimal) : Enabled
Report suppression : Enabled
TCN solicit query : Disabled
TCN flood query count : 2
Robustness variable : 2
Last member query count : 2
Last member query interval : 1000

Vlan 1:
-----
IGMP snooping : Enabled
IGMPv2 immediate leave : Disabled
Multicast router learning mode : pim-dvmrp
CGMP interoperability mode : IGMP_ONLY
Robustness variable : 2
Last member query count : 2
Last member query interval : 1000
```

The following is a sample output from the **show ip igmp snooping** command. It displays snooping characteristics for all the VLANs on the device:

```
Device# show ip igmp snooping

Global IGMP Snooping configuration:
-----
IGMP snooping : Enabled
IGMPv3 snooping (minimal) : Enabled
Report suppression : Enabled
TCN solicit query : Disabled
TCN flood query count : 2
Robustness variable : 2
Last member query count : 2
Last member query interval : 1000

Vlan 1:
-----
IGMP snooping : Enabled
IGMPv2 immediate leave : Disabled
Multicast router learning mode : pim-dvmrp
CGMP interoperability mode : IGMP_ONLY
Robustness variable : 2
Last member query count : 2
Last member query interval : 1000

Vlan 2:
-----
IGMP snooping : Enabled
IGMPv2 immediate leave : Disabled
Multicast router learning mode : pim-dvmrp
CGMP interoperability mode : IGMP_ONLY
Robustness variable : 2
```

```
Last member query count      : 2
Last member query interval   : 1000
-
.
.
.
```

show ip igmp snooping groups

To display the Internet Group Management Protocol (IGMP) snooping multicast table for the device or the multicast information, use the **show ip igmp snooping groups** command in privileged EXEC mode.

Command Modes	Privileged EXEC User EXEC
----------------------	------------------------------

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines	Expressions are case sensitive. For example, if you enter exclude output , the lines that contain "output" do not appear, but the lines that contain "Output" appear.
-------------------------	--

Examples

The following is a sample output from the **show ip igmp snooping groups** command without any keywords. It displays the multicast table for the device.

```
Device# show ip igmp snooping groups
Vlan      Group        Type      Version      Port List
-----+
1         224.1.4.4    igmp
1         224.1.4.5    igmp
2         224.0.1.40   igmp      v2
104       224.1.4.2   igmp      v2
104       224.1.4.3   igmp      v2
                                         Port List
                                         Gi1/0/11
                                         Gi1/0/11
                                         Gi1/0/15
                                         Gi2/0/1, Gi2/0/2
                                         Gi2/0/1, Gi2/0/2
```

The following is a sample output from the **show ip igmp snooping groups count** command. It displays the total number of multicast groups on the device.

```
Device# show ip igmp snooping groups count
```

```
Total number of multicast groups: 2
```

The following is a sample output from the **show ip igmp snooping groups vlan vlan-id ip-address** command. It shows the entries for the group with the specified IP address:

```
Device# show ip igmp snooping groups vlan 104 224.1.4.2
```

```
Vlan      Group        Type      Version      Port List
-----+
104       224.1.4.2   igmp      v2
                                         Port List
                                         Gi2/0/1, Gi1/0/15
```

show ip igmp snooping membership

show ip igmp snooping membership

To display IGMP host membership information, use the **show ip igmp snooping membership** command in the Privileged EXEC mode.

```
show ip igmp snooping membership [interface interface_num] [vlan vlan-id] [reporter a.b.c.d] [source a.b.c.d group a.b.c.d]
```

Syntax Description	interface <i>interface_num</i> vlan <i>vlan-id</i> reporter <i>a.b.c.d</i> source <i>a.b.c.d</i> group <i>a.b.c.d</i>	(Optional) Displays IP address and version information of an interface. (Optional) Displays VLAN members sorted by group IP address of a VLAN; valid values are from 1 to 1001 and from 1006 to 4094. (Optional) Displays membership information for a specified reporter. (Optional) Specifies a reporter, source, or group IP address. (Optional) Displays all members of a channel (source, group), that are sorted by an interface or a VLAN.
Command Default	None	
Command Modes	Privileged EXEC	
Command History	Release	Modification
	Cisco IOS XE Fuji 16.8.1a	This command was introduced.

Usage Guidelines This command is valid only if explicit host tracking is enabled on the switch.

Examples

The following example shows how to display host membership for the port channel 9:

```
Device# show ip igmp snooping membership interface port-channel 9
Source/Group    Interface Reporter    Vlan Uptime    Last-Join/ Last-Leave
-----
99.99.99.1/232.1.1.1    Po9 88.88.88.2        100   00:00:02    00:00:02 /
99.99.99.1/232.1.1.2    Po9 88.88.88.2        100   00:00:02    00:00:02 /
99.99.99.1/232.1.1.3    Po9 88.88.88.2        100   00:00:02    00:00:02 /
99.99.99.1/232.1.1.4    Po9 88.88.88.2        100   00:00:02    00:00:02 /
99.99.99.1/232.1.1.5    Po9 88.88.88.2        100   00:00:02    00:00:02 /
```

```

99.99.99.1/232.1.1.6 Po9 88.88.88.2 100 00:00:02 00:00:02 /
99.99.99.1/232.1.1.7 Po9 88.88.88.2 100 00:00:02 00:00:02 /
99.99.99.1/232.1.1.8 Po9 88.88.88.2 100 00:00:02 00:00:02 /
99.99.99.1/232.1.1.9 Po9 88.88.88.2 100 00:00:02 00:00:02 /
99.99.99.1/232.1.1.10 Po9 88.88.88.2 100 00:00:02 00:00:02 /
Device#

```

The following example shows how to display host membership for VLAN 100 and group 232.1.1.1 :

```

Device# show ip igmp snooping membership vlan 100 source 99.99.99.1 group 232.1.1.1
Source/Group      Interface Reporter   Vlan Uptime Last-Join/ Last-Leave
-----
99.99.99.1/232.1.1.1 Po9     88.88.88.2 100 00:00:28 00:00:28/
Device #

```

The following example shows how to display host membership information for VLAN 100 and to delete the explicit host tracking:

```

Device# show ip igmp snooping membership vlan 100
Snooping Membership Summary for Vlan 100
-----
Total number of channels: 10
Total number of hosts : 1
Source/Group      Interface Reporter   Vlan Uptime Last-Join/ Last-Leave
-----
99.99.99.1/232.1.1.1 Po9 88.88.88.2 100 00:00:02 00:00:02 /
99.99.99.1/232.1.1.2 Po9 88.88.88.2 100 00:00:02 00:00:02 /
99.99.99.1/232.1.1.3 Po9 88.88.88.2 100 00:00:02 00:00:02 /
99.99.99.1/232.1.1.4 Po9 88.88.88.2 100 00:00:02 00:00:02 /
99.99.99.1/232.1.1.5 Po9 88.88.88.2 100 00:00:02 00:00:02 /
99.99.99.1/232.1.1.6 Po9 88.88.88.2 100 00:00:02 00:00:02 /
99.99.99.1/232.1.1.7 Po9 88.88.88.2 100 00:00:02 00:00:02 /
99.99.99.1/232.1.1.8 Po9 88.88.88.2 100 00:00:02 00:00:02 /
99.99.99.1/232.1.1.9 Po9 88.88.88.2 100 00:00:02 00:00:02 /
99.99.99.1/232.1.1.10 Po9 88.88.88.2 100 00:00:02 00:00:02 /
Device#
Device#clear ip igmp snooping membership vlan 100

```

show ip igmp snooping mrouter

show ip igmp snooping mrouter

To display the Internet Group Management Protocol (IGMP) snooping dynamically learned and manually configured multicast router ports for the device or for the specified multicast VLAN, use the **show ip igmp snooping mrouter** command in privileged EXEC mode.

show ip igmp snooping mrouter [vlan *vlan-id*]

Syntax Description	vlan <i>vlan-id</i> (Optional) Specifies a VLAN; Ranges are from 1—1001 and 1006—4094.
---------------------------	---

Command Modes	User EXEC
----------------------	-----------

Privileged EXEC

Command History	Release	Modification
------------------------	----------------	---------------------

Cisco IOS XE Everest 16.6.1	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 device:

```
Device# show ip igmp snooping mrouter
Vlan      ports
----      -----
1        Gi2/0/1 (dynamic)
```

show ip igmp snooping querier

To display the configuration and operation information for the IGMP querier that is configured on a device, use the **show ip igmp snooping querier** command in user EXEC mode.

show ip igmp snooping querier [vlan *vlan-id*] [detail]

Syntax Description	vlan <i>vlan-id</i> (Optional) Specifies a VLAN; Ranges are from 1—1001 and 1006—4094.
---------------------------	---

detail	(Optional) Displays detailed IGMP querier information.
---------------	--

Command Modes	User EXEC Privileged EXEC				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				

Usage Guidelines Use the **show ip igmp snooping querier** command to display the IGMP version and the IP address of a detected device, also called a querier, that sends IGMP query messages. A subnet can have multiple multicast routers but only one IGMP querier. In a subnet running IGMPv2, one of the multicast routers is elected as the querier. The querier can be a Layer 3 device.

The **show ip igmp snooping querier** command output also shows the VLAN and the interface on which the querier was detected. If the querier is the device, the output shows the Port field as Router. If the querier is a router, the output shows the port number on which the querier was detected in the Port field.

The **show ip igmp snooping querier detail** user EXEC command is similar to the **show ip igmp snooping querier** command. However, the **show ip igmp snooping querier** command displays only the device IP address most recently detected by the device querier.

The **show ip igmp snooping querier detail** command displays the device IP address most recently detected by the device querier and this additional information:

- The elected IGMP querier in the VLAN
- The configuration and operational information pertaining to the device querier (if any) that is configured in the VLAN

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

Examples

The following is a sample output from the **show ip igmp snooping querier** command:

```
Device> show ip igmp snooping querier
Vlan      IP Address      IGMP Version      Port
-----
1        172.20.50.11    v3                  Gi1/0/1
2        172.20.40.20    v2                  Router
```

The following is a sample output from the **show ip igmp snooping querier detail** command:

```
Device> show ip igmp snooping querier detail
Vlan      IP Address      IGMP Version      Port
-----
1        1.1.1.1          v2                  Fa8/0/1
Global IGMP device querier status
-----
admin state           : Enabled
admin version         : 2
source IP address    : 0.0.0.0
query-interval (sec) : 60
max-response-time (sec) : 10
querier-timeout (sec) : 120
tcn query count      : 2
```

show ip pim autorp

```

tcn query interval (sec)      : 10
Vlan 1:   IGMP device querier status
-----
elected querier is 1.1.1.1      on port Fa8/0/1
-----
admin state                  : Enabled
admin version                : 2
source IP address            : 10.1.1.65
query-interval (sec)          : 60
max-response-time (sec)       : 10
querier-timeout (sec)         : 120
tcn query count               : 2
tcn query interval (sec)      : 10
operational state             : Non-Querier
operational version           : 2
tcn query pending count       : 0

```

show ip pim autorp

To display global information about auto-rp, use the **show ip pim autorp** command in privileged EXEC mode.

show ip pim autorp

Syntax Description This command has no arguments or keywords.

Command Default Auto RP is enabled by default.

Command Modes Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines This command displays whether auto-rp is enabled or disabled.

Example

The following command output shows that Auto RP is enabled:

```

Device# show ip pim autorp

AutoRP Information:
  AutoRP is enabled.
  RP Discovery packet MTU is 0.
  224.0.1.40 is joined on GigabitEthernet1/0/1.

PIM AutoRP Statistics: Sent/Received
  RP Announce: 0/0, RP Discovery: 0/0

```

show ip pim bsr-router

To display information related to Protocol Independent Multicast (PIM) bootstrap router (BSR) protocol processing, use the **show ip pim bsr-router** command in user EXEC or privileged EXEC mode.

show ip pim bsr-router

Syntax Description	This command has no arguments or keywords.	
Command Default	None	
Command Modes	User EXEC Privileged EXEC	
Command History		
Release	Modification	
Cisco IOS XE Everest 16.6.1	This command was introduced.	

Usage Guidelines In addition to Auto RP, the BSR RP method can be configured. After the BSR RP method is configured, this command displays the BSR router information.

The following is sample output from the **show ip pim bsr-router** command:

```
Device# show ip pim bsr-router

PIMv2 Bootstrap information
This system is the Bootstrap Router (BSR)
  BSR address: 172.16.143.28
  Uptime: 04:37:59, BSR Priority: 4, Hash mask length: 30
  Next bootstrap message in 00:00:03 seconds

Next Cand_RP_advertisement in 00:00:03 seconds.
  RP: 172.16.143.28(Ethernet0), Group acl: 6
```

show ip pim bsr

To display information related to Protocol Independent Multicast (PIM) bootstrap router (BSR) protocol processing, use the **show ip pim bsr** command in user EXEC or privileged EXEC mode.

show ip pim bsr

Syntax Description	This command has no arguments or keywords.	
Command Default	None	
Command Modes	User EXEC Privileged EXEC	

show ip pim snooping

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines	In addition to Auto RP, the BSR RP method can be configured. After the BSR RP method is configured, this command displays the BSR router information.
-------------------------	---

The following is sample output from the **show ip pim bsr** command:

```
Device# show ip pim bsr

PIMv2 Bootstrap information
This system is the Bootstrap Router (BSR)
  BSR address: 172.16.143.28
  Uptime: 04:37:59, BSR Priority: 4, Hash mask length: 30
  Next bootstrap message in 00:00:03 seconds

Next Cand_RP_advertisement in 00:00:03 seconds.
  RP: 172.16.143.28(Ethernet0), Group acl: 6
```

show ip pim snooping

To display the information about IP PIM snooping, use the **show ip pim snooping** command in user EXEC or privileged EXEC mode.

Global Status

show ip pim snooping

VLAN Status

show ip pim snooping vlan *vlan-id* [{neighbor | statistics | mroute [{source-ip|group-ip}]}]

Syntax Description	vlan <i>vlan-id</i> 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 Everest 16.6.1	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
```

show ip pim snooping

```

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 18: 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 <i>vrf-name</i> (Optional) Specifies a virtual routing and forwarding (VRF) configuration. Tunnel <i>interface-number</i> (Optional) Specifies the tunnel interface number. verbose (Optional) Provides additional information, such as the MAC encapsulation header and platform-specific information.
Command Default	None
Command Modes	Privileged EXEC
Command History	Release Modification Cisco IOS XE Everest 16.6.1 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.

show platform software fed switch ip multicast

The following syslog message appears when a PIM tunnel interface is created:

```
* %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel<interface_number>,  
changed state to up
```

The following is sample output from the **show ip pim tunnel** taken from an RP. The output is used to verify the PIM Encap and Decap Tunnel on the RP:

```
Device# show ip pim tunnel
```

```
Tunnel0  
  Type    : PIM Encap  
  RP      : 70.70.70.1*  
  Source  : 70.70.70.1  
Tunnel1*  
  Type    : PIM Decap  
  RP      : 70.70.70.1*  
  Source  : -R2#
```



Note The asterisk (*) indicates that the router is the RP. The RP will always have a PIM Encap and Decap Tunnel interface.

show platform software fed switch ip multicast

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. <ul style="list-style-type: none"> • 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.
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

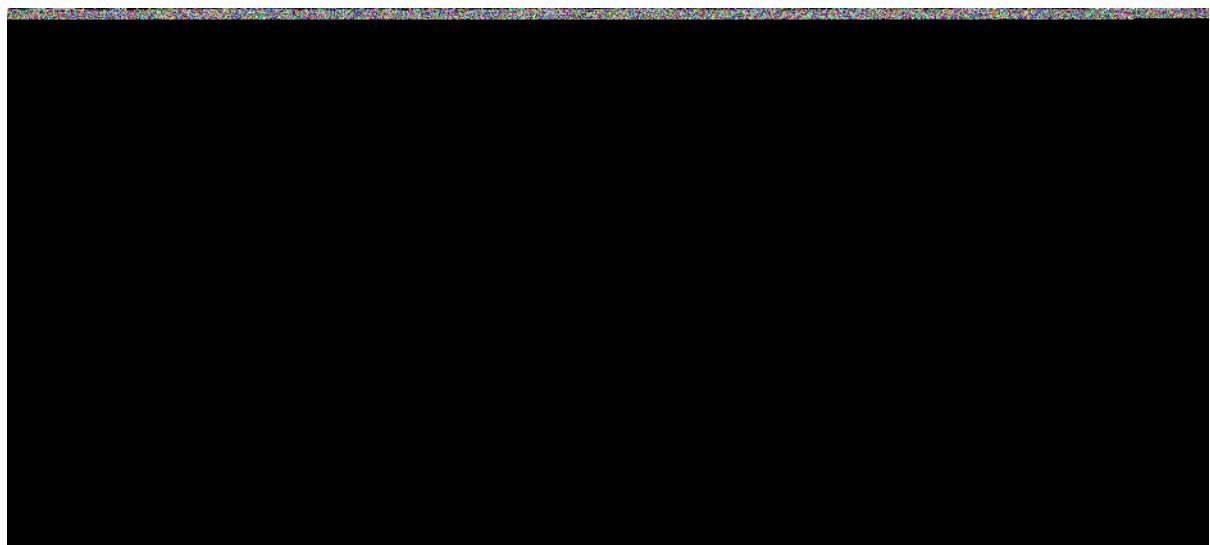
The following example shows how to display platform IP multicast routes per group:

```
show platform software fed switch ip multicast
```

```
al_rsc_di
RM:index = 0x51f6
RM:pmap = 0x0
RM:cni = 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_cni
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

IPv6

- [IPv6 Commands, on page 263](#)

IPv6 Commands

- [clear ipv6 access-list](#), on page 266
- [clear ipv6 dhcp](#), on page 267
- [clear ipv6 dhcp binding](#), on page 267
- [clear ipv6 dhcp client](#), on page 268
- [clear ipv6 dhcp conflict](#), on page 269
- [clear ipv6 dhcp relay binding](#), on page 270
- [clear ipv6 eigrp](#), on page 271
- [clear ipv6 mfib counters](#), on page 271
- [clear ipv6 mld counters](#), on page 272
- [clear ipv6 mld traffic](#), on page 273
- [clear ipv6 mtu](#), on page 273
- [clear ipv6 multicast aaa authorization](#), on page 274
- [clear ipv6 nd destination](#), on page 275
- [clear ipv6 nd on-link prefix](#), on page 275
- [clear ipv6 nd router](#), on page 276
- [clear ipv6 neighbors](#), on page 277
- [clear ipv6 nhrp](#), on page 278
- [clear ipv6 ospf](#), on page 279
- [clear ipv6 ospf counters](#), on page 280
- [clear ipv6 ospf events](#), on page 281
- [clear ipv6 pim reset](#), on page 282
- [clear ipv6 pim topology](#), on page 282
- [clear ipv6 pim traffic](#), on page 283
- [clear ipv6 prefix-list](#), on page 283
- [clear ipv6 rip](#), on page 284
- [clear ipv6 route](#), on page 285
- [clear ipv6 spd](#), on page 286
- [clear ipv6 traffic](#), on page 287
- [ipv6 access-list](#), on page 288
- [ipv6 cef](#), on page 291
- [ipv6 cef accounting](#), on page 292
- [ipv6 cef distributed](#), on page 294
- [ipv6 cef load-sharing algorithm](#), on page 295

- ipv6 cef optimize neighbor resolution, on page 296
- ipv6 destination-guard policy, on page 297
- ipv6 dhcp-relay bulk-lease, on page 297
- ipv6 dhcp-relay option vpn, on page 298
- ipv6 dhcp-relay source-interface, on page 299
- ipv6 dhcp binding track ppp, on page 300
- ipv6 dhcp database, on page 301
- ipv6 dhcp iana-route-add, on page 302
- ipv6 dhcp iapd-route-add, on page 303
- **ipv6 dhcp-ldra**, on page 303
- ipv6 dhcp ping packets, on page 304
- ipv6 dhcp pool, on page 305
- ipv6 flow monitor , on page 307
- ipv6 dhcp server vrf enable, on page 308
- ipv6 general-prefix, on page 308
- ipv6 local policy route-map, on page 310
- ipv6 local pool, on page 311
- ipv6 mld snooping, on page 312
- ipv6 mld ssm-map enable, on page 313
- ipv6 mld state-limit, on page 314
- ipv6 multicast-routing, on page 315
- ipv6 multicast group-range, on page 316
- ipv6 multicast pim-passive-enable, on page 317
- ipv6 multicast rpf, on page 318
- ipv6 nd cache expire, on page 319
- ipv6 nd cache interface-limit (global), on page 319
- ipv6 nd host mode strict, on page 320
- ipv6 nd ns-interval, on page 321
- ipv6 nd reachable-time, on page 322
- ipv6 nd resolution data limit, on page 323
- ipv6 nd route-owner, on page 324
- ipv6 neighbor, on page 325
- ipv6 ospf name-lookup, on page 326
- ipv6 pim, on page 327
- ipv6 pim accept-register, on page 328
- ipv6 pim allow-rp , on page 328
- ipv6 pim anycast-RP, on page 329
- ipv6 pim neighbor-filter list, on page 330
- ipv6 pim rp-address, on page 331
- ipv6 pim rp embedded, on page 333
- ipv6 pim spt-threshold infinity, on page 334
- ipv6 prefix-list, on page 334
- ipv6 source-guard attach-policy, on page 337
- ipv6 source-route, on page 338
- ipv6 spd mode, on page 339
- ipv6 spd queue max-threshold, on page 340

- [ipv6 traffic interface-statistics](#), on page 341
- [ipv6 unicast-routing](#), on page 341
- [show ipv6 access-list](#), on page 342
- [show ipv6 destination-guard policy](#), on page 344
- [show ipv6 dhcp](#), on page 345
- [show ipv6 dhcp binding](#), on page 346
- [show ipv6 dhcp conflict](#), on page 348
- [show ipv6 dhcp database](#), on page 349
- [show ipv6 dhcp guard policy](#), on page 350
- [show ipv6 dhcp interface](#), on page 352
- [show ipv6 dhcp relay binding](#), on page 354
- [show ipv6 eigrp events](#), on page 355
- [show ipv6 eigrp interfaces](#), on page 356
- [show ipv6 eigrp topology](#), on page 358
- [show ipv6 eigrp traffic](#), on page 360
- [show ipv6 general-prefix](#), on page 361
- [show ipv6 interface](#), on page 362
- [show ipv6 mfib](#), on page 369
- [show ipv6 mld groups](#), on page 375
- [show ipv6 mld interface](#), on page 377
- [show ipv6 mld snooping](#), on page 379
- [show ipv6 mld ssm-map](#), on page 380
- [show ipv6 mld traffic](#), on page 382
- [show ipv6 mrrib client](#), on page 383
- [show ipv6 mrrib route](#), on page 384
- [show ipv6 mroute](#), on page 386
- [show ipv6 mtu](#), on page 390
- [show ipv6 nd destination](#), on page 391
- [show ipv6 nd on-link prefix](#), on page 392
- [show ipv6 neighbors](#), on page 393
- [show ipv6 nhrp](#), on page 396
- [show ipv6 ospf](#), on page 399
- [show ipv6 ospf border-routers](#), on page 403
- [show ipv6 ospf event](#), on page 404
- [show ipv6 ospf graceful-restart](#), on page 406
- [show ipv6 ospf interface](#), on page 407
- [show ipv6 ospf request-list](#), on page 412
- [show ipv6 ospf retransmission-list](#), on page 413
- [show ipv6 ospf statistics](#), on page 414
- [show ipv6 ospf summary-prefix](#), on page 416
- [show ipv6 ospf timers rate-limit](#), on page 417
- [show ipv6 ospf traffic](#), on page 418
- [show ipv6 ospf virtual-links](#), on page 421
- [show ipv6 pim anycast-RP](#), on page 423
- [show ipv6 pim bsr](#), on page 423
- [show ipv6 pim df](#), on page 425

clear ipv6 access-list

- [show ipv6 pim group-map](#), on page 427
- [show ipv6 pim interface](#), on page 429
- [show ipv6 pim join-prune statistic](#), on page 430
- [show ipv6 pim limit](#), on page 431
- [show ipv6 pim neighbor](#), on page 432
- [show ipv6 pim range-list](#), on page 433
- [show ipv6 pim topology](#), on page 434
- [show ipv6 pim traffic](#), on page 436
- [show ipv6 pim tunnel](#), on page 438
- [show ipv6 policy](#), on page 439
- [show ipv6 prefix-list](#), on page 440
- [show ipv6 protocols](#), on page 442
- [show ipv6 rip](#), on page 445
- [show ipv6 route](#), on page 450
- [show ipv6 routers](#), on page 453
- [show ipv6 rpf](#), on page 456
- [show ipv6 source-guard policy](#), on page 458
- [show ipv6 spd](#), on page 458
- [show ipv6 static](#), on page 459
- [show ipv6 traffic](#), on page 462
- [show ipv6 pim tunnel](#), on page 465

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	<i>access-list-name</i> (Optional) Name of the IPv6 access list for which to clear the match counters. Names cannot contain a space or quotation mark, or begin with a numeric.				
Command Default	No reset is initiated.				
Command Modes	Privileged EXEC (#)				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				
Usage Guidelines	<p>The clear ipv6 access-list command is similar to the clear ip access-list counters command, except that it is IPv6-specific.</p> <p>The clear ipv6 access-list command used without the <i>access-list-name</i> argument resets the match counters for all IPv6 access lists configured on the router.</p>				

This command resets the IPv6 global ACL hardware counters.

Examples

The following example resets the match counters for the IPv6 access list named marketing:

```
Device# 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 Everest 16.6.1	This command was introduced.

Usage Guidelines

The **clear ipv6 dhcp** command deletes DHCP for IPv6 information.

Examples

The following example :

```
Device# clear ipv6 dhcp
```

clear ipv6 dhcp binding

To delete automatic client bindings from the Dynamic Host Configuration Protocol (DHCP) for IPv6 server binding table, use the **clear ipv6 dhcp binding** command in privileged EXEC mode.

```
clear ipv6 dhcp binding [ipv6-address] [vrf vrf-name]
```

clear ipv6 dhcp client

Syntax Description	<i>ipv6-address</i>	(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 <i>vrf-name</i>	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.

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

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	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:

```
Device# 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	<i>interface-type interface-number</i>	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 Everest 16.6.1	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:					
	<pre>Device# clear ipv6 dhcp client Ethernet 1/0</pre>					
Related Commands	<table border="1"> <thead> <tr> <th>Command</th><th>Description</th></tr> </thead> <tbody> <tr> <td>show ipv6 dhcp interface</td><td>Displays DHCP for IPv6 interface information.</td></tr> </tbody> </table>		Command	Description	show ipv6 dhcp interface	Displays DHCP for IPv6 interface information.
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.
	<i>ipv6-address</i>	Clears the host IPv6 address that contains the conflicting address.
	vrf <i>vrf-name</i>	Specifies a virtual routing and forwarding (VRF) name.

Command Modes	Privileged EXEC (#)	
Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

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.

clear ipv6 dhcp relay binding

If the **vrf vrf-name** keyword and argument are specified, only the address conflicts that belong to the specified VRF will be cleared.

Examples

The following example shows how to clear all address conflicts from the DHCPv6 server database:

```
Device# clear ipv6 dhcp conflict *
```

Related Commands	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.
	<i>ipv6-address</i>	DHCPv6 address.
	<i>ipv6-prefix</i>	IPv6 prefix.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	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:

```
Device# clear ipv6 dhcp relay binding 2001:0DB8:3333:4::5
```

The following example shows how to clear the binding for a client with the VRF name vrf1 and a specified prefix on a Cisco uBR10012 universal broadband device:

```
Device# clear ipv6 dhcp relay binding vrf vrf1 2001:DB8:0:1::/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

<i>as-number</i>	(Optional) Autonomous system number.
neighbor	(Optional) Deletes neighbor router entries.
<i>ipv6-address</i>	(Optional) IPv6 address of a neighboring router.
<i>interface-type</i>	(Optional) The interface type of the neighbor router.
<i>interface-number</i>	(Optional) The interface number of the neighbor router.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Everest 16.6.1	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-type**interface-number* argument, to remove a specific neighbor from the neighbor table.

Examples

The following example removes the neighbor whose IPv6 address is 3FEE:12E1:2AC1:EA32:

```
Device# clear ipv6 eigrp neighbor 3FEE:12E1:2AC1:EA32
```

clear ipv6 mfib counters

To reset all active Multicast Forwarding Information Base (MFIB) traffic counters, use the **clear ipv6 mfib counters** command in privileged EXEC mode.

clear ipv6 mfib [vrf *vrf-name*] counters [{group-name | group-address [{source-address source-name}]}]

Syntax Description

vrf <i>vrf-name</i>	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
----------------------------	--

clear ipv6 mld counters

<i>group-name group-address</i>	(Optional) IPv6 address or name of the multicast group.
<i>source-address source-name</i>	(Optional) IPv6 address or name of the source.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
Cisco IOS XE Everest 16.6.1		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:

```
Device# clear ipv6 mfib counters
```

clear ipv6 mld counters

To clear the Multicast Listener Discovery (MLD) interface counters, use the **clear ipv6 mld counters** command in privileged EXEC mode.

```
clear ipv6 mld [vrf vrf-name] counters [interface-type]
```

vrf <i>vrf-name</i>	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
<i>interface-type</i>	(Optional) Interface type. For more information, use the question mark (?) online help function.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
Cisco IOS XE Everest 16.6.1		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:

```
Device# 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 Everest 16.6.1	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:

```
Device# 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

clear ipv6 multicast aaa authorization

Syntax Description	This command has no arguments or keywords.				
Command Default	Messages are not cleared from the MTU cache.				
Command Modes	Privileged EXEC (#)				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	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:				
	<pre>Device# clear ipv6 mtu</pre>				
Related Commands	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>ipv6 flowset</td> <td>Configures flow-label marking in 1280-byte or larger packets sent by the router.</td> </tr> </tbody> </table>	Command	Description	ipv6 flowset	Configures flow-label marking in 1280-byte or larger packets sent by the router.
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	<i>interface-type interface-number</i>	Interface type and number. For more information, use the question mark (?) online help function.				
Command Modes	Privileged EXEC (#)					
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>		Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification					
Cisco IOS XE Everest 16.6.1	This command was introduced.					
Usage Guidelines	Using the clear ipv6 multicast aaa authorization command without the optional <i>interface-type</i> and <i>interface-number</i> arguments will clear all authorization parameters on a network.					
Examples	The following example clears all configured authorization parameters on an IPv6 network:					

```
Device# clear ipv6 multicast aaa authorization FastEthernet 1/0
```

Related Commands	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 Everest 16.6.1	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:
-----------------	--

```
Device# 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.
---------------------------	--

clear ipv6 nd router

Command Modes	Privileged EXEC (#)	
Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	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: Device# 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 Everest 16.6.1 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: Device# **clear ipv6 nd router** |

Device# **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 Everest 16.6.1	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:

```
Device# clear ipv6 neighbors
```

The following example clears all IPv6 neighbor discovery cache entries, except static entries and ND cache entries on non-VRF interfaces, on Ethernet interface 0/0:

clear ipv6 nhrp

```
Device# clear ipv6 neighbors interface Ethernet 0/0
```

The following example clears a neighbor discovery cache entry for 2001:0DB8:1::1 on Ethernet interface 0/0:

```
Device# clear ipv6 neighbors 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 nhrp

To clear all dynamic entries from the Next Hop Resolution Protocol (NHRP) cache, use the **clear ipv6 nhrp** command in privileged EXEC mode.

```
clear ipv6 nhrp [{ipv6-address | counters}]
```

Syntax Description

<i>ipv6-address</i>	(Optional) The IPv6 network to delete.
counters	(Optional) Specifies NHRP counters to delete.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines

This command does not clear any static (configured) IPv6-to-nonbroadcast multiaccess (NBMA) address mappings from the NHRP cache.

Examples

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

```
Device# clear ipv6 nhrp
```

Related Commands

Command	Description
show ipv6 nhrp	Displays the NHRP cache.

clear ipv6 ospf

To clear the Open Shortest Path First (OSPF) state based on the OSPF routing process ID, use the **clear ipv6 ospf** command in privileged EXEC mode.

```
clear ipv6 ospf [process-id] {process | force-spf | redistribution}
```

Syntax Description

<i>process-id</i>	(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 Everest 16.6.1	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 OSPF process. If the *process-id* option is not specified, all OSPF processes are cleared.

Examples

The following example starts the SPF algorithm without clearing the OSPF database:

```
Device# clear ipv6 ospf force-spf
```

clear ipv6 ospf counters

clear ipv6 ospf counters

To clear the Open Shortest Path First (OSPF) state based on the OSPF routing process ID, use the **clear ipv6 ospf** command in privileged EXEC mode.

clear ipv6 ospf [process-id] counters [neighbor [{neighbor-interface}neighbor-id}]

Syntax Description	<table border="1"> <tr> <td><i>process-id</i></td><td>(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when enabling the OSPF routing process.</td></tr> <tr> <td>neighbor</td><td>(Optional) Neighbor statistics per interface or neighbor ID.</td></tr> <tr> <td><i>neighbor-interface</i></td><td>(Optional) Neighbor interface.</td></tr> <tr> <td><i>neighbor-id</i></td><td>(Optional) IPv6 or IP address of the neighbor.</td></tr> </table>	<i>process-id</i>	(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.	<i>neighbor-interface</i>	(Optional) Neighbor interface.	<i>neighbor-id</i>	(Optional) IPv6 or IP address of the neighbor.
<i>process-id</i>	(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.								
<i>neighbor-interface</i>	(Optional) Neighbor interface.								
<i>neighbor-id</i>	(Optional) IPv6 or IP address of the neighbor.								

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	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:

```
Device# show ipv6 ospf neighbor detail
Neighbor 10.0.0.1
  In the area 1 via interface Serial19/0
  Neighbor:interface-id 21, link-local address FE80::A8BB:CCFF:FE00:6F00
  Neighbor priority is 1, State is FULL, 6 state changes
  Options is 0x194AE05
  Dead timer due in 00:00:37
  Neighbor is up for 00:00:15
  Index 1/1/1, retransmission queue length 0, number of retransmission 1
  First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
  Last retransmission scan length is 1, maximum is 1
  Last retransmission scan time is 0 msec, maximum is 0 msec
```

The following example clears all neighbors on the specified interface:

```
Device# clear ipv6 ospf counters neighbor s19/0
```

The following example now shows that there have been 0 state changes since the **clear ipv6 ospf counters neighbor s19/0** command was used:

```
Device# show ipv6 ospf neighbor detail
Neighbor 10.0.0.1
  In the area 1 via interface Serial19/0
  Neighbor:interface-id 21, link-local address FE80::A8BB:CCFF:FE00:6F00
  Neighbor priority is 1, State is FULL, 0 state changes
  Options is 0x194AE05
  Dead timer due in 00:00:39
  Neighbor is up for 00:00:43
  Index 1/1/1, retransmission queue length 0, number of retransmission 1
  First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
  Last retransmission scan length is 1, maximum is 1
  Last retransmission scan time is 0 msec, maximum is 0 msec
```

Related Commands

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 **clear ipv6 ospf events** command in privileged EXEC mode.

clear ipv6 ospf [process-id] events

Syntax Description

<i>process-id</i>	(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 Everest 16.6.1	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:

```
Device# clear ipv6 ospf 1 events
```

clear ipv6 pim reset

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	<table border="1"> <tr> <td>vrf vrf-name</td><td>(Optional) Specifies a virtual routing and forwarding (VRF) configuration.</td></tr> </table>	vrf vrf-name	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.		
vrf vrf-name	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.				
Command Modes	Privileged EXEC (#)				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	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:

```
Device# clear ipv6 pim reset
```

clear ipv6 pim topology

To clear the Protocol Independent Multicast (PIM) topology table, use the **clear ipv6 pim topology** command in privileged EXEC mode.

clear ipv6 pim [vrf vrf-name] topology [{group-name|group-address}]

Syntax Description	<table border="1"> <tr> <td>vrf vrf-name</td><td>(Optional) Specifies a virtual routing and forwarding (VRF) configuration.</td></tr> <tr> <td>group-name group-address</td><td>(Optional) IPv6 address or name of the multicast group.</td></tr> </table>	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.
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 Everest 16.6.1	This command was introduced.

Usage Guidelines This command clears PIM protocol information from all group entries located in the PIM topology table. Information obtained from the MRIB table is retained. If a multicast group is specified, only those group entries are cleared.

Examples The following example clears all group entries located in the PIM topology table:

```
Device# clear ipv6 pim topology
```

clear ipv6 pim traffic

To clear the Protocol Independent Multicast (PIM) traffic counters, use the **clear ipv6 pim traffic** command in privileged EXEC mode.

```
clear ipv6 pim [vrf vrf-name] traffic
```

Syntax Description	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 Everest 16.6.1	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:

```
Device# clear ipv6 pim traffic
```

clear ipv6 prefix-list

To reset the hit count of the IPv6 prefix list entries, use the **clear ipv6 prefix-list** command in privileged EXEC mode.

```
clear ipv6 prefix-list [prefix-list-name] [ipv6-prefix/prefix-length]
```

clear ipv6 rip

Syntax Description	<p><i>prefix-list-name</i> (Optional) The name of the prefix list from which the hit count is to be cleared.</p> <p><i>ipv6-prefix</i> (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.</p> <p><i>/ prefix-length</i> (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.</p>
---------------------------	--

Command Default The hit count is automatically cleared for all IPv6 prefix lists.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	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`.

```
Device# 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	<i>name</i>	(Optional) Name of an IPv6 RIP process.
	vrf <i>vrf-name</i>	(Optional) Clears information about the specified Virtual Routing and Forwarding (VRF) instance.

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

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	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:

```
Device# clear ipv6 rip one
```

The following example deletes the IPv6 VRF instance, called vrf1 for the RIP process, called one:

```
Device# clear ipv6 rip one vrf vrf1
```

```
*Mar 15 12:36:17.022: 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-address/ipv6-prefix/prefix-length} | *}
```

clear ipv6 spd

Syntax Description	<p><i>ipv6-address</i></p> <p>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.</p> <p><i>ipv6-prefix</i></p> <p>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.</p> <p>/ <i>prefix-length</i></p> <p>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.</p> <p>*</p> <p>Clears all IPv6 routes.</p>
---------------------------	--

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	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:

```
Device# 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 Everest 16.6.1	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:

```
Device# clear ipv6 spd
```

clear ipv6 traffic

To reset IPv6 traffic counters, use the **clear ipv6 traffic** command in privileged EXEC mode.

clear ipv6 traffic [interface-type interface-number]

Syntax Description	<i>interface-type interface-number</i>	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 Everest 16.6.1	This command was introduced.

Usage Guidelines Using this command resets the counters in the output from the **show ipv6 traffic** command.

Examples The following example resets the IPv6 traffic counters. The output from the **show ipv6 traffic** command shows that the counters are reset:

```
Device# clear ipv6 traffic
Device# show ipv6 traffic
IPv6 statistics:
Rcvd: 1 total, 1 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 router
      0 fragments, 0 total reassembled
      0 reassembly timeouts, 0 reassembly failures
Sent: 1 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: 1 input, 0 checksum errors, 0 too short
      0 unknown info type, 0 unknown error type
```

ipv6 access-list

```

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 router solicit, 0 router advert, 0 redirects
0 neighbor solicit, 1 neighbor advert
Sent: 1 output
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 router solicit, 0 router advert, 0 redirects
0 neighbor solicit, 1 neighbor advert
UDP statistics:
Rcvd: 0 input, 0 checksum errors, 0 length errors
0 no port, 0 dropped
Sent: 0 output
TCP statistics:
Rcvd: 0 input, 0 checksum errors
Sent: 0 output, 0 retransmitted

```

Related Commands

Command	Description
show ipv6 traffic	Displays IPv6 traffic statistics.

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

<i>access-list-name</i>	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 Everest 16.6.1	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.

ipv6 access-list

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 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 Everest 16.6.1	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 Device.

```
Device(config)# ip cef
Device(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	<p><i>accounting-types</i></p> <p>The <i>accounting-types</i> 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.</p> <ul style="list-style-type: none"> • 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	<p>Enables accounting through nonrecursive prefixes.</p> <p>This keyword is optional when used in global configuration mode after another keyword is entered. See the <i>accounting-types</i> argument.</p>
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 Everest 16.6.1	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

ipv6 cef distributed

contains a path to use. The source and destination IP addresses are the properties used to select the bucket for per-destination load balancing. Use the **load-balance-hash** keyword with the **ipv6 cef accounting** command to enable per-hash-bucket counters. Enter the **show ipv6 cef prefix internal** command to display the per-hash-bucket counters.

Examples

The following example enables the collection of Cisco Express Forwarding for IPv6 accounting information for prefixes with directly connected next hops:

```
Device(config)# ipv6 cef accounting non-recursive
```

Related Commands

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 Everest 16.6.1	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:

```
Device(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.
<i>id</i>	(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 router automatically generates a unique ID.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced.

ipv6 cef optimize neighbor resolution**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(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 Everest 16.6.1	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:

```
Device(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	<i>policy-name</i> (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 Everest 16.6.1	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:

```
Device(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]

ipv6 dhcp-relay option vpn

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)

Release	Modification
Cisco IOS XE Everest 16.6.1	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:

```
Device(config)# ipv6 dhcp-relay bulk-lease data-timeout 60
```

ipv6 dhcp-relay option vpn

To enable the DHCP for IPv6 relay VRF-aware feature, use the **ipv6 dhcp-relay option vpn** command in global configuration mode. To disable the feature, use the **no** form of this command.

```
ipv6 dhcp-relay option vpn
no ipv6 dhcp-relay option vpn
```

Syntax Description This command has no arguments or keywords.

Command Default The DHCP for IPv6 relay VRF-aware feature is not enabled on the router.

Command Modes Global configuration (config)

Release	Modification
Cisco IOS XE Everest 16.6.1	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 router. 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 router:

```
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

<i>interface-type</i> <i>interface-number</i>	(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 Everest 16.6.1	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:

```
Device(config)# ipv6 dhcp-relay source-interface loopback 0
```

ipv6 dhcp binding track ppp

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 Everest 16.6.1	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:

```
Device(config)# ipv6 dhcp binding track ppp
```

ipv6 dhcp database

To configure a Dynamic Host Configuration Protocol (DHCP) for IPv6 binding database agent, use the **ipv6 dhcp database** command in global configuration mode. To delete the database agent, use the **no** form of this command.

```
 ipv6 dhcp database agent [write-delay seconds] [timeout seconds]
 no ipv6 dhcp database agent
```

Syntax Description	<i>agent</i>	A flash, local bootflash, compact flash, NVRAM, FTP, TFTP, or Remote Copy Protocol (RCP) uniform resource locator.
	write-delay <i>seconds</i>	(Optional) How often (in seconds) DHCP for IPv6 sends database updates. The default is 300 seconds. The minimum write delay is 60 seconds.
	timeout <i>seconds</i>	(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 Everest 16.6.1	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 aborted. By default, the DHCP for IPv6 server waits 300 seconds before aborting a database transfer. When the system is going to reload, there is no transfer timeout so that the binding table can be stored completely.

Examples

The following example specifies DHCP for IPv6 binding database agent parameters and stores binding entries in TFTP:

ipv6 dhcp iana-route-add

```
Device(config)# ipv6 dhcp database tftp://10.0.0.1/dhcp-binding
```

The following example specifies DHCP for IPv6 binding database agent parameters and stores binding entries in bootflash:

```
Device(config)# ipv6 dhcp database bootflash
```

Related Commands

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 Everest 16.6.1	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 Everest 16.6.1		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 router does not mean that routes will be added on that router. 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)

ipv6 dhcp ping packets

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	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	<p>The following example shows how to enable the LDRA functionality:</p> <pre>Device(config)# ipv6 dhcp-ldra enable Device(config)# exit</pre>	

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 *number*

Syntax Description	<i>number</i>	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 Everest 16.6.1	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:

```
Device(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

<i>poolname</i>	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 Everest 16.6.1	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:

```
Device(config)# ipv6 dhcp pool cisco1
Device(config-dhcpv6) #
```

The following example shows how to configure an IPv6 address prefix for the IPv6 configuration pool **cisco1**:

```
Device(config-dhcpv6) # address prefix 2001:1000::0/64
Device(config-dhcpv6) # end
```

The following example shows how to configure a pool named **engineering** with three link-address prefixes and an IPv6 address prefix:

```
Device# configure terminal
Device(config)# ipv6 dhcp pool engineering
Device(config-dhcpv6) # link-address 2001:1001::0/64
Device(config-dhcpv6) # link-address 2001:1002::0/64
Device(config-dhcpv6) # link-address 2001:2000::0/48
Device(config-dhcpv6) # address prefix 2001:1003::0/64
Device(config-dhcpv6) # end
```

The following example shows how to configure a pool named **350** with vendor-specific options:

```

Device# configure terminal
Device(config)# ipv6 dhcp pool 350
Device(config-dhcpv6)# vendor-specific 9
Device(config-dhcpv6-vs)# suboption 1 address 1000:235D::1Device(config-dhcpv6-vs)# suboption
2 ascii "IP-Phone"
Device(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 flow monitor

This command activates a previously created flow monitor by assigning it to the interface to analyze incoming or outgoing traffic.

To activate a previously created flow monitor, use the **ipv6 flow monitor** command. To de-activate a flow monitor, use the **no** form of the command.

```

ipv6 flow monitor ipv6-monitor-name [sampler ipv6-sampler-name] {input | output}
no ipv6 flow monitor ipv6-monitor-name [sampler ipv6-sampler-name] {input | output}

```

Syntax Description

<i>ipv6-monitor-name</i>	Activates a previously created flow monitor by assigning it to the interface to analyze incoming or outgoing traffic.
sampler <i>ipv6-sampler-name</i>	Applies the flow monitor sampler.
input	Applies the flow monitor on input traffic.
output	Applies the flow monitor on output traffic.

Command Default

IPv6 flow monitor is not activated until it is assigned to an interface.

Command Modes

Interface configuration (config-if)

Command History**Release** **Modification**

Cisco IOS XE Everest 16.6.1 This command was introduced.

Usage Guidelines

You cannot attach a NetFlow monitor to a port channel interface. If both service module interfaces are part of an EtherChannel, you should attach the monitor to both physical interfaces.

This example shows how to apply a flow monitor to an interface:

```

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

```

ipv6 dhcp server vrf enable

```
Device(config-if)# end
```

ipv6 dhcp server vrf enable

To enable the DHCP for IPv6 server VRF-aware feature, use the **ipv6 dhcp server vrf enable** command in global configuration mode. To disable the feature, use the **no** form of this command.

```
ipv6 dhcp server vrf enable
no ipv6 dhcp server vrf enable
```

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

Command Default	The DHCPv6 server VRF-aware feature is not enabled.
------------------------	---

Command Modes	Global configuration (config)
----------------------	-------------------------------

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines	The ipv6 dhcp server option vpn command allows the DHCPv6 server VRF-aware feature to be enabled globally on a device.
-------------------------	---

Examples	The following example enables the DHCPv6 server VRF-aware feature globally on a device:
-----------------	---

```
Device(config)# ipv6 dhcp server option vpn
```

ipv6 general-prefix

To define an IPv6 general prefix, use the **ipv6 general-prefix** command in global configuration mode. To remove the IPv6 general prefix, use the **no** form of this command.

```
ipv6 general-prefix prefix-name {ipv6-prefix/prefix-length | 6to4 interface-type interface-number | 6rd interface-type interface-number}
no ipv6 general-prefix prefix-name
```

Syntax Description	<table border="1"> <tr> <td><i>prefix-name</i></td><td>The name assigned to the prefix.</td></tr> <tr> <td><i>ipv6-prefix</i></td><td> 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 <i>ipv6-prefix</i> and <i>/prefix-length</i> arguments. </td></tr> </table>	<i>prefix-name</i>	The name assigned to the prefix.	<i>ipv6-prefix</i>	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 <i>ipv6-prefix</i> and <i>/prefix-length</i> arguments.
<i>prefix-name</i>	The name assigned to the prefix.				
<i>ipv6-prefix</i>	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 <i>ipv6-prefix</i> and <i>/prefix-length</i> arguments.				

<i>/ prefix-length</i>	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 <i>ipv6-prefix</i> and <i>/ prefix-length</i> 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 <i>interface-type interface-number</i> argument.
<i>interface-type interface-number</i>	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 <i>interface-type interface-number</i> 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 Everest 16.6.1	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*:

```
Device(config)# ipv6 general-prefix my-prefix 2001:DB8:2222::/48
```

The following example defines an IPv6 general prefix named *my-prefix* based on a 6to4 interface:

```
Device(config)# ipv6 general-prefix my-prefix 6to4 ethernet0
```

Related Commands	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	<i>route-map-name</i> Name of the route map to be used for local IPv6 PBR. The name must match a <i>route-map-name</i> value specified by the route-map command.								
Command Default	IPv6 packets are not policy routed.								
Command Modes	Global configuration (config)								
Command History	<table border="1"> <thead> <tr> <th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td><td>This command was introduced.</td></tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.				
Release	Modification								
Cisco IOS XE Everest 16.6.1	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: <pre>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</pre>								
Related Commands	<table border="1"> <thead> <tr> <th>Command</th><th>Description</th></tr> </thead> <tbody> <tr> <td>ipv6 policy route-map</td><td>Configures IPv6 PBR on an interface.</td></tr> <tr> <td>match ipv6 address</td><td>Specifies an IPv6 access list to be used to match packets for PBR for IPv6.</td></tr> <tr> <td>match length</td><td>Bases policy routing on the Level 3 length of a packet.</td></tr> </tbody> </table>	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								
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	<i>poolname</i>	User-defined name for the local prefix pool.
<i>prefix</i>	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.	
<i>/ prefix-length</i>	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).	
<i>assigned-length</i>	Length of prefix, in bits, assigned to the user from the pool. The value of the <i>assigned-length</i> argument cannot be less than the value of the <i>/ prefix-length</i> argument.	
shared	(Optional) Indicates that the pool is a shared pool.	
cache-size <i>size</i>	(Optional) Specifies the size of the cache.	

Command Default No pool is configured.

Command Modes Global configuration (global)

ipv6 mld snooping

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	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:
	<pre>Device(config)# ipv6 local pool pool1 2001:0DB8::/29 64 Device(config)# end Device# show ipv6 local pool Pool Prefix Free In use pool1 2001:0DB8::/29 65516 20</pre>

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

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 Everest 16.6.1	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:

```
Device(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 Everest 16.6.1	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.

ipv6 mld state-limit**Examples**

The following example shows how to enable the SSM mapping feature:

```
Device(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 Everest 16.6.1	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:

```
Device(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 Everest 16.6.1	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:

```
Device(config)# ipv6 multicast-routing
```

Related Commands	Command	Description
	ipv6 pim rp-address	Configures the address of a PIM RP for a particular group range.

ipv6 multicast group-range

Command	Description
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 Everest 16.6.1	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 mrouting states are created, no Protocol Independent Multicast (PIM) joins are forwarded), and drops data traffic on all interfaces in the system, thus disabling multicast for denied groups or channels.

Using the **ipv6 multicast group-range** global configuration command is equivalent to configuring the MLD access control and multicast boundary commands on all interfaces in the system. However, the **ipv6 multicast group-range** command can be overridden on selected interfaces by using the following interface configuration commands:

- **ipv6 mld access-group** *access-list-name*
- **ipv6 multicast boundary scope** *scope-value*

Because the **no ipv6 multicast group-range** command returns the router to its default configuration, existing multicast deployments are not broken.

Examples

The following example ensures that the router disables multicast for groups or channels denied by an access list named list2:

```
Device(config)# ipv6 multicast group-range list2
```

The following example shows that the command in the previous example is overridden on an interface specified by int2:

```
Device(config)# interface int2
Device(config-if)# ipv6 mld access-group 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 Everest 16.6.1	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:

ipv6 multicast rpf

```
Device(config)# ipv6 multicast pim-passive-enable
```

Related Commands

Command	Description
ipv6 pim passive	Configures PIM passive mode on a specific interface.

ipv6 multicast rpf

To enable IPv6 multicast reverse path forwarding (RPF) check to use Border Gateway Protocol (BGP) unicast routes in the Routing Information Base (RIB), use the **ipv6 multicast rpf** command in global configuration mode. To disable this function, use the **no** form of this command.

```
ipv6 multicast [vrf vrf-name] rpf {backoff initial-delay max-delay | use-bgp}
no ipv6 multicast [vrf vrf-name] rpf {backoff initial-delay max-delay | use-bgp}
```

Syntax Description

vrf vrf-name	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
backoff	Specifies the backoff delay after a unicast routing change.
<i>initial-delay</i>	Initial RPF backoff delay, in milliseconds (ms). The range is from 200 to 65535.
<i>max-delay</i>	Maximum RPF backoff delay, in ms. The range is from 200 to 65535.
use-bgp	Specifies to use BGP routes for multicast RPF lookups.

Command Default

The multicast RPF check does not use BGP unicast routes.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines

When the **ipv6 multicast rpf** command is configured, multicast RPF check uses BGP unicast routes in the RIB. This is not done by default.

Examples

The following example shows how to enable the multicast RPF check function:

```
Device(config)# ipv6 multicast rpf use-bgp
```

Related Commands

Command	Description
ipv6 multicast limit	Configure per-interface multicast route (mroute) state limiters in IPv6.
ipv6 multicast multipath	Enables load splitting of IPv6 multicast traffic across multiple equal-cost paths.

ipv6 nd cache expire

To configure the length of time before an IPv6 neighbor discovery (ND) cache entry expires, use the **ipv6 nd cache expire** command in 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	<table border="1"> <tr> <td><i>expire-time-in-seconds</i></td><td>The time range is from 1 through 65536 seconds. The default is 14400 seconds, or 4 hours.</td></tr> <tr> <td>refresh</td><td>(Optional) Automatically refreshes the ND cache entry.</td></tr> </table>	<i>expire-time-in-seconds</i>	The time range is from 1 through 65536 seconds. The default is 14400 seconds, or 4 hours.	refresh	(Optional) Automatically refreshes the ND cache entry.
<i>expire-time-in-seconds</i>	The time range is from 1 through 65536 seconds. The default is 14400 seconds, or 4 hours.				
refresh	(Optional) Automatically refreshes the ND cache entry.				

Command Default This expiration time is 14400 seconds (4 hours)

Command Modes Interface configuration (config-if)

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines By default, an ND 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 user to vary the expiry time and to trigger autorefresh of an expired entry before the entry is deleted.

When the **refresh** keyword is used, an ND cache entry is autorefreshed. The entry moves into the DELAY state and the neighbor unreachability detection (NUD) 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 (NS) is sent and then retransmitted as per the configuration.

Examples The following example shows that the ND cache entry is configured to expire in 7200 seconds, or 2 hours:

```
Device(config-if)# ipv6 nd cache expire 7200
```

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]
```

ipv6 nd host mode strict

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 Everest 16.6.1	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:

```
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 Everest 16.6.1	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:

```
Device(config)# ipv6 nd host mode strict
Device(config-if)# interface ethernet0/0
Device(config-if)# ipv6 address autoconfig
```

The following example shows how to configure the device as a strict IPv6 host and configures a static IPv6 address on Ethernet interface 0/0:

```
Device(config)# ipv6 nd host mode strict
Device(config-if)# interface ethernet0/0
Device(config-if)# ipv6 address 2001::1/64
```

Related Commands

Command	Description
ipv6 unicast-routing	Enables the forwarding of IPv6 unicast datagrams.

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

<i>milliseconds</i>	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)

ipv6 nd reachable-time

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines	<p>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.</p> <p>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.</p>
Examples	The following example configures an IPv6 neighbor solicit transmission interval of 9000 milliseconds for Ethernet interface 0/0:

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 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 Everest 16.6.1	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:

```
Device(config)# interface ethernet 0/0
Device(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

<i>number-of-packets</i>	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 Everest 16.6.1	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

ipv6 nd route-owner

packet loss generally is not a cause for concern. (Note that dropping the initial packet to an unresolved destination is normal in IPv4.) However, there may be some high-scale configurations where loss of the initial packet is inconvenient. In these cases, the customer can use the **ipv6 nd resolution data limit** command to prevent the initial packet loss by increasing the unresolved packet queue size.

Examples

The following example configures the global number of data packets held awaiting resolution to be 32:

```
Device(config)# ipv6 nd resolution data limit 32
```

ipv6 nd route-owner

To insert Neighbor Discovery-learned routes into the routing table with "ND" status and to enable ND autoconfiguration behavior, use the **ipv6 nd route-owner** command. To remove this information from the routing table, use the **no** form of this command.

ipv6 ndroute-owner

Syntax Description

This command has no arguments or keywords.

Command Default

The status of Neighbor Discovery-learned routes is "Static."

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Everest 16.6.1	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

```
Device(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	<table border="1"> <tr> <td><i>ipv6-address</i></td><td>The IPv6 address that corresponds to the local data-link address. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.</td></tr> <tr> <td><i>interface-type</i></td><td>The specified interface type. For supported interface types, use the question mark (?) online help function.</td></tr> <tr> <td><i>interface-number</i></td><td>The specified interface number.</td></tr> <tr> <td><i>hardware-address</i></td><td>The local data-link address (a 48-bit address).</td></tr> </table>	<i>ipv6-address</i>	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.	<i>interface-type</i>	The specified interface type. For supported interface types, use the question mark (?) online help function.	<i>interface-number</i>	The specified interface number.	<i>hardware-address</i>	The local data-link address (a 48-bit address).
<i>ipv6-address</i>	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.								
<i>interface-type</i>	The specified interface type. For supported interface types, use the question mark (?) online help function.								
<i>interface-number</i>	The specified interface number.								
<i>hardware-address</i>	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 Everest 16.6.1	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

ipv6 ospf name-lookup

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 INCMPI).

Static entries in the IPv6 neighbor discovery cache are not modified by the neighbor discovery process.



Note Static entries for IPv6 neighbors can be configured only on IPv6-enabled LAN and ATM LAN Emulation interfaces.

Examples

The following example configures a static entry in the IPv6 neighbor discovery cache for a neighbor with the IPv6 address 2001:0DB8::45A and link-layer address 0002.7D1A.9472 on Ethernet interface 1:

```
Device(config)# ipv6 neighbor 2001:0DB8::45A ethernet1 0002.7D1A.9472
```

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 Everest 16.6.1	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)# 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 Everest 16.6.1	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:

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

ipv6 pim accept-register

To accept or reject registers at the rendezvous point (RP), use the **ipv6 pim accept-register** command in global configuration mode. To return to the default value, use the **no** form of this command.

```
ipv6 pim [vrf vrf-name] accept-register {list access-list | route-map map-name}
no ipv6 pim [vrf vrf-name] accept-register {list access-list | route-map map-name}
```

Syntax Description	<table border="1"> <tr> <td>vrf <i>vrf-name</i></td><td>(Optional) Specifies a virtual routing and forwarding (VRF) configuration.</td></tr> <tr> <td>list <i>access-list</i></td><td>Defines the access list name.</td></tr> <tr> <td>route-map <i>map-name</i></td><td>Defines the route map.</td></tr> </table>	vrf <i>vrf-name</i>	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.	list <i>access-list</i>	Defines the access list name.	route-map <i>map-name</i>	Defines the route map.
vrf <i>vrf-name</i>	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.						
list <i>access-list</i>	Defines the access list name.						
route-map <i>map-name</i>	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 Everest 16.6.1	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 Border Gateway Protocol (BGP) prefix:

```
ipv6 pim accept-register route-map reg-filter
route-map reg-filter permit 20
  match as-path 101
  ip as-path access-list 101 permit
```

ipv6 pim allow-rp

To enable the PIM Allow RP feature for all IP multicast-enabled interfaces in an IPv6 device, use the **ip pim allow-rp** command in global configuration mode. To return to the default value, use the **no** form of this command.

```
ipv6 pim allow-rp [{group-list access-list | rp-list access-list [group-list access-list]}]
no ipv6 pim allow-rp
```

Syntax Description	<table border="1"> <tr> <td>group-list</td><td>(Optional) Identifies an access control list (ACL) of allowed group ranges for PIM Allow RP.</td></tr> </table>	group-list	(Optional) Identifies an access control list (ACL) of allowed group ranges for PIM Allow RP.
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.
<i>access-list</i>	(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 Everest 16.6.1	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 anycast-RP

To configure the address of the Protocol-Independent Multicast (PIM) rendezvous point (RP) for an anycast group range, use the **ipv6 pim anycast-RP** command in global configuration mode. To remove an RP address for an anycast group range, use the **no** form of this command.

ipv6 pim anycast-RP {rp-address peer-address}
no ipv6 pim anycast-RP

Syntax Description	<i>anycast-rp-address</i>	Anycast RP set for the RP assigned to the group range. This is the address that first-hop and last-hop PIM routers use to register and join.
	<i>peer-address</i>	The address to which register messages copies are sent. This address is any address assigned to the RP router, not including the address assigned using the <i>anycast-rp-address</i> variable.

Command Default No PIM RP address is configured for an anycast group range.

Command Modes Global configuration (config)

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

ipv6 pim neighbor-filter list**Usage Guidelines**

The anycast RP feature is useful when interdomain connection is not required. Use this command to configure the address of the PIM RP for an anycast group range.

Examples

```
Device# ipv6 pim anycast-rp 2001:DB8::1:1 2001:DB8::3:3
```

Related Commands

Command	Description
show ipv6 pim anycast-RP	Verifies IPv6 PIM RP anycast configuration.

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 Everest 16.6.1	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:

```
Device(config)# ipv6 pim neighbor-filter list nbr_filter_acl
Device(config)# ipv6 access-list nbr_filter_acl
Device(config-ipv6-acl)# deny ipv6 host FE80::A8BB:CCFF:FE03:7200 any
Device(config-ipv6-acl)# permit any any
```

ipv6 pim rp-address

To configure the address of a Protocol Independent Multicast (PIM) rendezvous point (RP) for a particular group range, use the **ipv6 pim rp-address** command in global configuration mode. To remove an RP address, use the **no** form of this command.

```
ipv6 pim [vrf vrf-name] rp-address ipv6-address [group-access-list] [bidir]
no ipv6 pim rp-address ipv6-address [group-access-list] [bidir]
```

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 <i>ipv6-address</i> 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 Everest 16.6.1		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

ipv6 pim rp-address

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:

```
Device(config)# ipv6 pim rp-address 2001::10:10
```

The following example sets the PIM RP address to 2001::10:10 for the multicast group FF04::/64 only:

```
Device(config)# ipv6 access-list acc-grp-1
Device(config-ipv6-acl)# permit ipv6 any ff04::/64
Device(config)# ipv6 pim rp-address 2001::10:10 acc-grp-1
```

The following example shows how to configure a group access list that permits the embedded RP ranges derived from the IPv6 RP address 2001:0DB8:2::2:

```
Device(config)# ipv6 pim rp-address 2001:0DB8:2::2 embd-ranges
Device(config)# ipv6 access-list embd-ranges
Device(config-ipv6-acl)# permit ipv6 any ff73:240:2:2:2::/96
Device(config-ipv6-acl)# permit ipv6 any ff74:240:2:2:2::/96
Device(config-ipv6-acl)# permit ipv6 any ff75:240:2:2:2::/96
Device(config-ipv6-acl)# permit ipv6 any ff76:240:2:2:2::/96
Device(config-ipv6-acl)# permit ipv6 any ff77:240:2:2:2::/96
Device(config-ipv6-acl)# permit ipv6 any ff78:240:2:2:2::/96
```

The following example shows how to enable the address 100::1 as the bidirectional RP for the entries multicast range FF::/8:

```
ipv6 pim rp-address 100::1 bidir
```

In the following example, the IPv6 address 200::1 is enabled as the bidirectional RP for the ranges permitted by the access list named bidir-grps. The ranges permitted by this list are ff05::/16 and ff06::/16.

```
Device(config)# ipv6 access-list bidir-grps
Device(config-ipv6-acl)# permit ipv6 any ff05::/16
Device(config-ipv6-acl)# permit ipv6 any ff06::/16
Device(config-ipv6-acl)# exit
Device(config)# ipv6 pim rp-address 200::1 bidir-grps bidir
```

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 Everest 16.6.1	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:

```
Device# no ipv6 pim rp embedded
```

■ **ipv6 pim spt-threshold infinity**

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	<table border="1"> <tr> <td>vrf <i>vrf-name</i></td><td>(Optional) Specifies a virtual routing and forwarding (VRF) configuration.</td></tr> <tr> <td>group-list <i>access-list-name</i></td><td>(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.</td></tr> </table>	vrf <i>vrf-name</i>	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.	group-list <i>access-list-name</i>	(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.
vrf <i>vrf-name</i>	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.				
group-list <i>access-list-name</i>	(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 Everest 16.6.1	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.:

```
Device(config)# ipv6 access-list acc-grp-1
Device(config-ipv6-acl)# permit ipv6 any FF04::/64
Device(config-ipv6-acl)# exit
Device(config)# ipv6 pim spt-threshold infinity group-list acc-grp-1
```

ipv6 prefix-list

To create an entry in an IPv6 prefix list, use the **ipv6 prefix-list** command in global configuration mode. To delete the entry, use the **no** form of this command.

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	<p><i>list-name</i> Name of the prefix list.</p> <ul style="list-style-type: none"> • 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 <i>seq-number</i>	(Optional) Sequence number of the prefix list entry being configured.
deny	Denies networks that matches the condition.
permit	Permits networks that matches the condition.
<i>ipv6-prefix</i>	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.
<i>/prefix-length</i>	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 <i>text</i>	A description of the prefix list that can be up to 80 characters in length.
ge <i>ge-value</i>	(Optional) Specifies a prefix length greater than or equal to the <i>ipv6-prefix/prefix-length</i> arguments. It is the lowest value of a range of the <i>length</i> (the “from” portion of the length range).
le <i>le-value</i>	(Optional) Specifies a prefix length less than or equal to the <i>ipv6-prefix /prefix-length</i> arguments. It is the highest value of a range of the <i>length</i> (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 Everest 16.6.1	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.

ipv6 prefix-list

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.

```
Device(config)# ipv6 prefix-list abc deny ::/0
```

The following example permits the prefix 2002::/16:

```
Device(config)# ipv6 prefix-list abc permit 2002::/16
```

The following example shows how to specify a group of prefixes to accept any prefixes from prefix 5F00::/48 up to and including prefix 5F00::/64.

```
Device(config)# ipv6 prefix-list abc permit 5F00::/48 le 64
```

The following example denies prefix lengths greater than 64 bits in routes that have the prefix 2001:0DB8::/64.

```
Device(config)# ipv6 prefix-list abc permit 2001:0DB8::/64 le 128
```

The following example permits mask lengths from 32 to 64 bits in all address space.

```
Device(config)# ipv6 prefix-list abc permit ::/0 ge 32 le 64
```

The following example denies mask lengths greater than 32 bits in all address space.

```
Device(config)# ipv6 prefix-list abc deny ::/0 ge 32
```

The following example denies all routes with a prefix of 2002::/128.

```
Device(config)# ipv6 prefix-list abc deny 2002::/128
```

The following example permits all routes with a prefix of ::/0.

```
Device(config)# ipv6 prefix-list abc permit ::/0
```

Related Commands

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	<i>source-guard-policy</i> (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 Everest 16.6.1	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.

ipv6 source-route

A dependency exists between IPv6 source guard and IPv6 snooping. Whenever IPv6 source guard is configured, when the **ipv6 source-guard attach-policy** command is entered, it verifies that snooping is enabled and issues a warning if it is not. If IPv6 snooping is disabled, the software checks if IPv6 source guard is enabled and sends a warning if it is.

Examples

The following example shows how to apply IPv6 source guard on an interface:

```
Device(config)# interface gigabitethernet 0/0/1
Device(config-if)# ipv6 source-guard attach-policy mysnoopingpolicy
```

Related Commands

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 Everest 16.6.1	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.
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 Everest 16.6.1	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

ipv6 spd queue max-threshold

enters max state, in which normal priority packets are discarded. If the input queue is between the minimum and maximum thresholds, SPD enters the random drop state, in which normal packets may be dropped.

Examples

The following example shows how to enable the router to drop deformed packets when the router is in the random drop state:

```
Device(config)# ipv6 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	<i>value</i> 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 Everest 16.6.1	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:

```
Device(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 Everest 16.6.1	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:

```
Device(config)# ipv6 traffic interface-statistics unclearable
```

ipv6 unicast-routing

To enable the forwarding of IPv6 unicast datagrams, use the **ipv6 unicast-routing** command in global configuration mode. To disable the forwarding of IPv6 unicast datagrams, use the **no** form of this command.

```
ipv6 unicast-routing
no ipv6 unicast-routing
```

show ipv6 access-list

Syntax Description	This command has no arguments or keywords.												
Command Default	IPv6 unicast routing is disabled.												
Command Modes	Global configuration (config)												
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.								
Release	Modification												
Cisco IOS XE Everest 16.6.1	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:												
<pre>Device(config)# ipv6 unicast-routing</pre>													
Related Commands	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>ipv6 address link-local</td> <td>Configures an IPv6 link-local address for an interface and enables IPv6 processing on the interface.</td> </tr> <tr> <td>ipv6 address eui-64</td> <td>Configures an IPv6 address and enables IPv6 processing on an interface using an EUI-64 interface ID in the low-order 64 bits of the address.</td> </tr> <tr> <td>ipv6 enable</td> <td>Enables IPv6 processing on an interface that has not been configured with an explicit IPv6 address.</td> </tr> <tr> <td>ipv6 unnumbered</td> <td>Enables IPv6 processing on an interface without assigning an explicit IPv6 address to the interface.</td> </tr> <tr> <td>show ipv6 route</td> <td>Displays the current contents of the IPv6 routing table.</td> </tr> </tbody> </table>	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.
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.												

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	<i>access-list-name</i> (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 Everest 16.6.1	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:

```
Device# show ipv6 access-list
IPv6 access list inbound
    permit tcp any any eq bgp reflect tcptraffic (8 matches) sequence 10
    permit tcp any any eq telnet reflect tcptraffic (15 matches) sequence 20
    permit udp any any reflect udptraffic sequence 30
IPv6 access list tcptraffic (reflexive) (per-user)
    permit tcp host 2001:0DB8:1::1 eq bgp host 2001:0DB8:1::2 eq 11000 timeout 300 (time
        left 243) sequence 1
    permit tcp host 2001:0DB8:1::1 eq telnet host 2001:0DB8:1::2 eq 11001 timeout 300
        (time left 296) sequence 2
IPv6 access list outbound
    evaluate udptraffic
    evaluate tcptraffic
```

The following sample output shows IPv6 access list information for use with IPSec:

```
Device# show ipv6 access-list
IPv6 access list Tunnel0-head-0-ACL (crypto)
    permit ipv6 any any (34 matches) sequence 1
IPv6 access list Ethernet2/0-ipsecv6-ACL (crypto)
    permit 89 FE80::/10 any (85 matches) sequence 1
```

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

Table 19: show ipv6 access-list Field Descriptions

Field	Description
ipv6 access list inbound	Name of the IPv6 access list, for example, inbound.
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.
bgp	Border Gateway Protocol. The lower-level (Layer 3) protocol type that the packet must be equal to.
reflect	Indicates a reflexive IPv6 access list.

show ipv6 destination-guard policy

Field	Description
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	<i>policy-name</i>	(Optional) Name of the destination guard policy.
--------------------	--------------------	--

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

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	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:

```
Device# 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:

```
Device# 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 Everest 16.6.1	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

show ipv6 dhcp binding

network interface is assumed to be permanently attached to the device. Use the **show ipv6 dhcp** command to display the DUID of a device.

Examples

The following is sample output from the **show ipv6 dhcp** command. The output is self-explanatory:

```
Device# show ipv6 dhcp
This device's DHCPv6 unique identifier (DUID): 000300010002FCA5DC1C
```

show ipv6 dhcp binding

To display automatic client bindings from the Dynamic Host Configuration Protocol (DHCP) for IPv6 server binding table, use the **show ipv6 dhcp binding** command in user EXEC or privileged EXEC mode.

show ipv6 dhcp binding [ipv6-address] [vrf vrf-name]

Syntax Description	<i>ipv6-address</i> (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 Everest 16.6.1	This command was introduced.

Usage Guidelines The **show ipv6 dhcp binding** command displays all automatic client bindings from the DHCP for IPv6 server binding table if the *ipv6-address* argument is not specified. When the *ipv6-address* argument is specified, only the binding for the specified client is displayed.

If the **vrf vrf-name** keyword and argument combination is specified, all bindings that belong to the specified VRF are displayed.



Note The **ipv6 dhcp server vrf enable** command must be enabled for the configured VRF to work. If the command is not configured, the output of the **show ipv6 dhcp binding** command will not display the configured VRF; it will only display the default VRF details.

Examples

The following sample output displays all automatic client bindings from the DHCP for IPv6 server binding table:

```
Device# show ipv6 dhcp binding
Client: FE80::A8BB:CCFF:FE00:300
        DUID: 00030001AABBCC000300
```

```

Username : client_1
Interface: Virtual-Access2.1
IA PD: IA ID 0x000C0001, T1 75, T2 135
Prefix: 2001:380:E00::/64
    preferred lifetime 150, valid lifetime 300
    expires at Dec 06 2007 12:57 PM (262 seconds)
Client: FE80::A8BB:CCFF:FE00:300 (Virtual-Access2.2)
DUID: 00030001AABBCC000300
IA PD: IA ID 0x000D0001, T1 75, T2 135
Prefix: 2001:0DB8:E00:1::/64
    preferred lifetime 150, valid lifetime 300
    expires at Dec 06 2007 12:58 PM (288 seconds)

```

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

Table 20: 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":

```
Device# show ipv6 dhcp binding
```

show ipv6 dhcp conflict

```

Client: FE80::2AA:FF:FEBB:CC
DUID: 0003000100AA00BB00CC
Username : client_1
Interface : Virtual-Access2
IA PD: IA ID 0x00130001, T1 75, T2 135
Prefix: 2001:0DB8:1:3::/80
    preferred lifetime 150, valid lifetime 300
    expires at Aug 07 2008 05:19 AM (225 seconds)

```

The following example shows that the PPP username associated with the binding is unassigned:

```

Device# show ipv6 dhcp binding

Client: FE80::2AA:FF:FEBB:CC
DUID: 0003000100AA00BB00CC
Username : unassigned
Interface : Virtual-Access2
IA PD: IA ID 0x00130001, T1 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	<i>ipv6-address</i> (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 Everest 16.6.1	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.:

```
Device# 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

<i>agent-URL</i>	(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 Everest 16.6.1	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:

```
Device# show ipv6 dhcp database
Database agent tftp://172.19.216.133/db.tftp:
    write delay: 69 seconds, transfer timeout: 300 seconds
    last written at Jan 09 2003 01:54 PM,
        write timer expires in 56 seconds
    last read at Jan 06 2003 05:41 PM
    successful read times 1
    failed read times 0
    successful write times 3172
```

show ipv6 dhcp guard policy

```

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 21: 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 aborting a database transfer. Transfers that exceed the timeout period are aborted.
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	<i>policy-name</i> (Optional) DHCPv6 guard policy name.
---------------------------	---

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

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines	If the <i>policy-name</i> argument is specified, only the specified policy information is displayed. If the <i>policy-name</i> argument is not specified, information is displayed for all policies.
-------------------------	--

Examples	The following is sample output from the show ipv6 dhcp guard command:
-----------------	--

```
Device# show ipv6 dhcp guard policy

Dhcp guard policy: default
    Device Role: dhcp client
    Target: Et0/3

Dhcp guard policy: test1
    Device Role: dhcp server
    Target: vlan 0     vlan 1     vlan 2     vlan 3     vlan 4
    Max Preference: 200
    Min Preference: 0
    Source Address Match Access List: acl1
    Prefix List Match Prefix List: pfxlist1

Dhcp guard policy: test2
    Device Role: dhcp relay
    Target: Et0/0 Et0/1 Et0/2
```

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

Table 22: 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

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	<i>type number</i> (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 Everest 16.6.1	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:

```
Device# show ipv6 dhcp interface
Ethernet2/1 is in server mode
  Using pool: svr-p1
  Preference value: 20
  Rapid-Commit is disabled
Router2# show ipv6 dhcp interface
Ethernet2/1 is in client mode
  State is OPEN (1)
  List of known servers:
    Address: FE80::202:FCFF:FEA1:7439, DUID 000300010002FCA17400
    Preference: 20
      IA PD: IA ID 0x00040001, T1 120, T2 192
        Prefix: 3FFE:C00:C18:1::/72
          preferred lifetime 240, valid lifetime 54321
          expires at Nov 08 2002 09:10 AM (54319 seconds)
        Prefix: 3FFE:C00:C18:2::/72
          preferred lifetime 300, valid lifetime 54333
          expires at Nov 08 2002 09:11 AM (54331 seconds)
        Prefix: 3FFE:C00:C18:3::/72
          preferred lifetime 280, valid lifetime 51111
          expires at Nov 08 2002 08:17 AM (51109 seconds)
    DNS server: 1001::1
    DNS server: 1001::2
    Domain name: domain1.net
    Domain name: domain2.net
    Domain name: domain3.net
```

```
Prefix name is cli-p1
Rapid-Commit is enabled
```

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

Table 23: 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:

```
Device(config-if)# ipv6 dhcp relay destination FE80::250:A2FF:FEBF:A056 FastEthernet0/1
Device# show ipv6 dhcp interface FastEthernet 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

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 <i>vrf-name</i> (Optional) Specifies a virtual routing and forwarding (VRF) configuration.
---------------------------	---

Command Modes User EXEC (>)

Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	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 24: show ipv6 dhcp relay binding Field Descriptions

Field	Description
Prefix	IPv6 prefix for DHCP.
DUID	DHCP Unique Identifier (DUID) for the IPv6 relay binding.

Field	Description
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.

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.
<i>event-num-start</i>	(Optional) Starting number of the event range. The range is from 1 to 4294967295.
<i>event-num-end</i>	(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 Everest 16.6.1	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.

```
Device# show ipv6 eigrp events
```

show ipv6 eigrp interfaces

```

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

<i>as-number</i>	(Optional) Autonomous system number.
<i>type</i>	(Optional) Interface type. For more information, use the question mark (?) online help function.
<i>number</i>	(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 Everest 16.6.1		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:

```
Device# 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:

```
Device# 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 mccasts: 0/20 Un/reliable uccasts: 31/398
```

show ipv6 eigrp topology

```
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 25: 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	
<i>as-number</i>	(Optional) Autonomous system number.
<i>ipv6-address</i>	(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 Everest 16.6.1	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.

```
Device# show ipv6 eigrp topology

IPv6-EIGRP Topology Table for AS(1)/ID(2001:0DB8:10::/64)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status
P 2001:0DB8:3::/64, 1 successors, FD is 281600
via Connected, Ethernet1/0
```

The following sample output from the **show ipv6 eigrp topology prefix** command displays ECMP mode information when the **no ipv6 next-hop-self** command is configured without the **no-ecmp-mode** option in the EIGRP topology. The ECMP mode provides information about the path that is being advertised. If there is more than one successor, the top most path will be advertised as the default path over all interfaces, and the message “ECMP Mode: Advertise by default” will be displayed in the output. If any path other than the default path is advertised, the message “ECMP Mode: Advertise out <Interface name>” will be displayed. The fields in the display are self-explanatory.

```
Device# show ipv6 eigrp topology 2001:DB8:10::1/128

EIGRP-IPv6 Topology Entry for AS(1)/ID(192.0.2.100) for 2001:DB8:10::1/128
  State is Passive, Query origin flag is 1, 2 Successor(s), FD is 284160
  Descriptor Blocks:
    FE80::A8BB:CCFF:FE01:2E01 (Tunnel0), from FE80::A8BB:CCFF:FE01:2E01, Send flag is 0x0
      Composite metric is (284160/281600), route is Internal
      Vector metric:
        Minimum bandwidth is 10000 Kbit
        Total delay is 1100 microseconds
        Reliability is 255/255
        Load is 255
        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 255
        Minimum MTU is 1400
        Hop count is 1
```

show ipv6 eigrp traffic

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

<i>as-number</i>	(Optional) Autonomous system number.
------------------	--------------------------------------

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Everest 16.6.1	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:

```
Device# show ipv6 eigrp traffic
IPv6-EIGRP Traffic Statistics for process 9
Hellos sent/received: 218/205
Updates sent/received: 7/23
Queries sent/received: 2/0
Replies sent/received: 0/2
Acks sent/received: 21/14
```

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

Table 26: 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.

Field	Description
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 Everest 16.6.1	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.

```
Device# show ipv6 general-prefix
IPv6 Prefix my-prefix, acquired via 6to4
2002:B0B:B0B::/48
Loopback42 (Address command)
```

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

Table 27: show ipv6 general-prefix Field Descriptions

Field	Description
IPv6 Prefix	User-defined name of the IPv6 general prefix.

show ipv6 interface

Field	Description
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.
<i>type</i>	(Optional) The interface type about which to display information.
<i>number</i>	(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 Everest 16.6.1	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.

```
Device(config)# show ipv6 interface ethernet0/0
Ethernet0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::A8BB:CCFF:FE00:6700
    No Virtual link-local address(es):
    Global unicast address(es):
      2001::1, subnet is 2001::/64 [DUP]
      2001::A8BB:CCFF:FE00:6700, subnet is 2001::/64 [EUI]
      2001:100::1, subnet is 2001:100::/64
    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 28: 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."

show ipv6 interface

Field	Description
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).
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.

Attribute	Description
DEP	Deprecated. The timed address is deprecated.
DUP	Duplicate. The address is a duplicate, as determined by duplicate address detection (DAD). To re-attempt 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.
OOD	Overly optimistic DAD. DAD will not be performed for this address. This attribute applies to virtual addresses.
PRE	Preferred. The timed address is preferred.
TEN	Tentative. The address is in a tentative state per DAD.
UNA	Unactivated. The virtual address is not active and is in a standby state.
VIRT	Virtual. The address is virtual and is managed by HSRP, VRRP, or GLBP.

show ipv6 interface Command Using the brief Keyword

The following is sample output from the **show ipv6 interface** command when entered with the **brief** keyword:

```
Device# show ipv6 interface brief
Ethernet0 is up, line protocol is up
  Ethernet0          [up/up]
    unassigned
  Ethernet1          [up/up]
    2001:0DB8:1000:/29
  Ethernet2          [up/up]
    2001:0DB8:2000:/29
  Ethernet3          [up/up]
    2001:0DB8:3000:/29
  Ethernet4          [up/down]
    2001:0DB8:4000:/29
  Ethernet5          [administratively down/down]
    2001:123::210:7BFF:FEC2:ACD8
    Interface      Status        IPv6 Address
    Ethernet0      up           3FFE:C00:0:1:260:3EFF:FE11:6770
    Ethernet1      up           unassigned
    Fddi0          up           3FFE:C00:0:2:260:3EFF:FE11:6772
    Serial10       administratively down unassigned
    Serial11       administratively down unassigned
    Serial12       administratively down unassigned
    Serial13       administratively down unassigned
    Tunnel0        up           unnumbered (Ethernet0)
    Tunnel1        up           3FFE:700:20:1::12
```

show ipv6 interface

IPv6 Interface with ND Prefix Configured

This sample output shows the characteristics of an interface that has generated a prefix from a local IPv6 prefix pool:

```
Device# show ipv6 interface Ethernet 0/0 prefix

interface Ethernet0/0
  ipv6 address 2001:0DB8::1/64
  ipv6 address 2001:0DB8::2/64
  ipv6 nd prefix 2001:0DB8:2::/64
  ipv6 nd prefix 2001:0DB8:3::/64 2592000 604800 off-link
end
.
.
.

IPv6 Prefix Advertisements Ethernet0/0
Codes: A - Address, P - Prefix-Advertisement, O - Pool
      U - Per-user prefix, D - Default
      N - Not advertised, C - Calendar
      default [LA] Valid lifetime 2592000, preferred lifetime 604800
AD 2001:0DB8:1::/64 [LA] Valid lifetime 2592000, preferred lifetime 604800
APD 2001:0DB8:2::/64 [LA] Valid lifetime 2592000, preferred lifetime 604800
P 2001:0DB8:3::/64 [A] Valid lifetime 2592000, preferred lifetime 604800
```

The default prefix shows the parameters that are configured using the `ipv6 nd prefix default` command.

IPv6 Interface with DRP Configured

This sample output shows the state of the DRP preference value as advertised by this device through an interface:

```
Device# show ipv6 interface gigabitethernet 0/1
GigabitEthernet0/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::130
  Description: Management network (dual stack)
  Global unicast address(es):
    FEC0:240:104:1000::130, subnet is FEC0:240:104:1000::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:130
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Low
  Hosts use stateless autoconfig for addresses.
```

IPv6 Interface with HSRP Configured

When HSRP IPv6 is first configured on an interface, the interface IPv6 link-local address is marked unactive (UNA) because it is no longer advertised, and the HSRP IPv6 virtual link-local address is added to the virtual link-local address list with the UNA and tentative DAD (TEN) attributes set. The interface is also programmed to listen for the HSRP IPv6 multicast address.

This sample output shows the status of UNA and TEN attributes, when HSRP IPv6 is configured on an interface:

```
Device# show ipv6 interface ethernet 0/0
Ethernet0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80:2::2 [UNA]
  Virtual link-local address(es):
    FE80::205:73FF:FEA0:1 [UNA/TEN]
  Global unicast address(es):
    2001:2::2, subnet is 2001:2::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::66
    FF02::1:FF00:2
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ND DAD is enabled, number of DAD attempts: 1
```

After the HSRP group becomes active, the UNA and TEN attributes are cleared, and the overly optimistic DAD (OOD) attribute is set. The solicited node multicast address for the HSRP virtual IPv6 address is also added to the interface.

This sample output shows the status of UNA, TEN and OOD attributes, when HSRP group is activated:

```
# show ipv6 interface ethernet 0/0
Ethernet0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80:2::2 [UNA]
  Virtual link-local address(es):
    FE80::205:73FF:FEA0:1 [OPT]
  Global unicast address(es):
    2001:2::2, subnet is 2001:2::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::66
    FF02::1:FF00:2
    FF02::1:FFA0:1
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 1
```

The table below describes additional significant fields shown in the displays for the **show ipv6 interface** command with HSRP configured.

Table 29: 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.

show ipv6 interface

Field	Description
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:

```
Device(config-if)# ipv6 nd ra-interval 100 60
```

Subsequent use of the **show ipv6 interface** then displays the interval as follows:

```
Device(config)# show ipv6 interface ethernet 1/0
Ethernet1/0 is administratively down, line protocol is down
  IPv6 is enabled, link-local address is FE80::A8BB:CCFF:FE00:5A01 [TEN]
  No Virtual link-local address(es):
  No global unicast address is configured
  Joined group address(es):
    FF02::1
    FF02::2
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 60 to 100 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.
```

In the following example, the maximum RA interval is configured as 100 milliseconds (ms), and the minimum RA interval is configured as 60 ms on Ethernet interface 1/0:

```
Device(config)# show ipv6 interface ethernet 1/0
Ethernet1/0 is administratively down, line protocol is down
  IPv6 is enabled, link-local address is FE80::A8BB:CCFF:FE00:5A01 [TEN]
  No Virtual link-local address(es):
  No global unicast address is configured
  Joined group address(es):
    FF02::1
```

```

FF02::2
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ICMP unreachables are sent
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 60 to 100 milliseconds
ND router advertisements live for 1800 seconds
ND advertised default router preference is Medium
Hosts use stateless autoconfig for addresses.

```

The table below describes additional significant fields shown in the displays for the **show ipv6 interface** command with minimum RA interval information configured.

Table 30: 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.
--------------	--

show ipv6 mfib

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.
<i>ipv6-prefix</i>	(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.
<i>/ prefix-length</i>	(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.
<i>group-address-name</i>	(Optional) IPv6 address or name of the multicast group.
<i>source-address-name</i>	(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 Everest 16.6.1	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 31: 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.

Flag	Description
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:

```
Device# show ipv6 mfib
IP Multicast Forwarding Information Base
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, D - Drop
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Interface Flags: A - Accept, F - Forward, NS - Negate Signalling
                 IC - Internal Copy, NP - Not platform switched
                 SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count
(*,FF00::/8) Flags: C
                    Forwarding: 0/0/0/0, Other: 0/0/0
                    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 32: 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.

show ipv6 mfib

Field	Description
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:

```
Device# show ipv6 mfib FF03:1::1
IP Multicast Forwarding Information Base
Entry Flags:C - Directly Connected, S - Signal, IA - Inherit A
flag,
          AR - Activity Required, D - Drop
Forwarding Counts:Pkt Count/Pkts per second/Avg Pkt Size/Kbits per
second
Other counts:Total/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:

```
Device# 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:

```

Device# 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:
  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:

```

Device# show ipv6 mfib FFE0::/15
IP Multicast Forwarding Information Base
Entry Flags:C - Directly Connected, S - Signal, IA - Inherit A flag,
          AR - Activity Required, D - Drop
Forwarding Counts:Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts:Total/RPF failed/Other drops
Interface Flags:A - Accept, F - Forward, NS - Negate Signalling
          IC - Internal Copy, NP - Not platform switched
          SP - Signal Present
Interface Counts:FS Pkt Count/PS Pkt Count

```

show ipv6 mfib

```
(*,:FFE0::/15) Flags:D
    Forwarding:0/0/0/0, Other:0/0/0
```

The following example shows output of the **show ipv6 mfib** command used with the **verbose** keyword. It shows forwarding entries and interfaces in the MFIB and additional information such as the MAC encapsulation header and platform-specific information.

```
Device# show ipv6 mfib ff33::1:1 verbose
IP Multicast Forwarding Information Base
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, K - Keepalive
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Platform per slot HW-Forwarding Counts: Pkt Count/Byte Count
Platform flags: HF - Forwarding entry,HB - Bridge entry,HD - NonRPF Drop entry,
                 NP - Not platform switchable,RPL - RPF-ltl linkage,
                 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: 33330001000100D0FFE180086DD
```

The table below describes the fields shown in the display.

Table 33: 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.
	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-name|group-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.
	<i>group-name group-address</i>	(Optional) IPv6 address or name of the multicast group.
	<i>interface-type interface-number</i>	(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 Everest 16.6.1	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.

```
Device# show ipv6 mld groups FastEthernet 2/1
MLD Connected Group Membership
Group Address          Interface      Uptime      Expires
FF02::2                FastEthernet2/1  3d18h     never
FF02::D                FastEthernet2/1  3d18h     never
FF02::16               FastEthernet2/1  3d18h     never
FF02::1:FF00:1          FastEthernet2/1  3d18h     00:00:27
FF02::1:FF00:79         FastEthernet2/1  3d18h     never
FF02::1:FF23:83C2       FastEthernet2/1  3d18h     00:00:22
FF02::1:FFAF:2C39       FastEthernet2/1  3d18h     never
FF06:7777::1            FastEthernet2/1  3d18h     00:00:26
```

The following is sample output from the **show ipv6 mld groups** command using the **detail** keyword:

show ipv6 mld groups

```
Device# 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:

```
Device# show ipv6 mld groups explicit
Ethernet1/0, FF05::1
Up:00:43:11 EXCLUDE(0/1) Exp:00:03:17
Host Address           Uptime   Expires
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 mode)
Exp:Expiry time for the group.
FE80::A8BB:CCFF:FE00:800 - Host ipv6 address.
00:43:11 - Uptime for the host.
00:03:17 - Expiry time for the host
Mode:INCLUDE/EXCLUDE - Mode the Host is operating in.
300::1, 300::2, 300::3 - Sources that the host has joined in the above specified mode.
```

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

Table 34: 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 Everest 16.6.1	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:

```
Device# show ipv6 mld interface Ethernet 2/1/1
Global State Limit : 2 active out of 2 max
Loopback0 is administratively down, line protocol is down
  Internet address is ::/0
.
.
.
Ethernet2/1/1 is up, line protocol is up
  Internet address is FE80::260:3EFF:FE86:5649/10
  MLD is enabled on interface
  Current MLD version is 2
  MLD query interval is 125 seconds
  MLD querier timeout is 255 seconds
  MLD max query response time is 10 seconds
```

show ipv6 mld interface

```
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 35: show ipv6 mld interface Field Descriptions

Field	Description
Global State Limit: 2 active out of 2 max	Two globally configured MLD states are active.
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.

Command	Description
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 <i>vlan-id</i> (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 Everest 16.6.1	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.

```
Device# show ipv6 mld snooping vlan 100
Global MLD Snooping configuration:
-----
MLD snooping : Enabled
MLDv2 snooping (minimal) : Enabled
Listener message suppression : Enabled
TCN solicit query : Disabled
TCN flood query count : 2
Robustness variable : 3
Last listener query count : 2
Last listener query interval : 1000
Vlan 100:
-----
MLD snooping : Disabled
MLDv1 immediate leave : Disabled
Explicit host tracking : Enabled
Multicast router learning mode : pim-dvmrp
Robustness variable : 3
```

show ipv6 mld ssm-map

```
Last listener query count : 2
Last listener query interval : 1000
```

This is an example of output from the **show ipv6 mld snooping** command. It displays snooping characteristics for all VLANs on the switch.

```
Device# show ipv6 mld snooping
Global MLD Snooping configuration:
-----
MLD snooping : Enabled
MLDv2 snooping (minimal) : Enabled
Listener message suppression : Enabled
TCN solicit query : Disabled
TCN flood query count : 2
Robustness variable : 3
Last listener query count : 2
Last listener query interval : 1000

Vlan 1:
-----
MLD snooping : Disabled
MLDv1 immediate leave : Disabled
Explicit host tracking : Enabled
Multicast router learning mode : pim-dvmrp
Robustness variable : 1
Last listener query count : 2
Last listener query interval : 1000

<output truncated>

Vlan 951:
-----
MLD snooping : Disabled
MLDv1 immediate leave : Disabled
Explicit host tracking : Enabled
Multicast router learning mode : pim-dvmrp
Robustness variable : 3
Last listener query count : 2
Last listener query interval : 1000
```

Related Commands	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.
--------------------	--------------	--

<i>source-address</i>	(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 Everest 16.6.1		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:

```
Device# show ipv6 mld ssm-map
SSM Mapping : Enabled
DNS Lookup : Enabled
```

The following examples show SSM mapping for the source address 2001:0DB8::1:

```
Device# show ipv6 mld ssm-map 2001:0DB8::1
Group address : 2001:0DB8::1
Group mode ssm : TRUE
Database : STATIC
Source list : 2001:0DB8::2
               2001:0DB8::3
Router# show ipv6 mld ssm-map 2001:0DB8::2
Group address : 2001:0DB8::2
Group mode ssm : TRUE
Database : DNS
Source list : 2001:0DB8::3
               2001:0DB8::1
```

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

Table 36: show ipv6 mld ssm-map Field Descriptions

Field	Description
SSM Mapping	The SSM mapping feature is enabled.
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.

show ipv6 mld traffic

Field	Description
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 Everest 16.6.1	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.

```
Device# show ipv6 mld traffic

MLD Traffic Counters
Elapsed time since counters cleared:00:00:21
          Received      Sent
Valid MLD Packets        3          1
Queries                  1          0
Reports                  2          1
Leaves                   0          0
```

Mtrace packets	0	0
Errors:		
Malformed Packets	0	
Bad Checksums	0	
Martian source	0	
Packets Received on MLD-disabled Interface	0	

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

Table 37: 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.
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).
	<i>client-name : client-id</i>	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 (#)

show ipv6 mrib route

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	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:

```
Device# show ipv6 mrib client
IP MRIB client-connections
igmp:145      (connection id 0)
pim:146       (connection id 1)
mfib ipv6:3   (connection id 2)
slot 3 mfib ipv6 rp agent:16  (connection id 3)
slot 1 mfib ipv6 rp agent:16  (connection id 4)
slot 0 mfib ipv6 rp agent:16  (connection id 5)
slot 4 mfib ipv6 rp agent:16  (connection id 6)
slot 2 mfib ipv6 rp agent:16  (connection id 7)
```

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

Table 38: 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-address source-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.

<i>prefix-length</i>	(Optional) IPv6 prefix length.
----------------------	--------------------------------

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Everest 16.6.1	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 39: 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
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)

show ipv6 mroute

- Source Specific Multicast (SSM) groups (FF3X::/32).

For all the remaining (usually sparse-mode) IPv6 multicast groups, a directly connected check is performed and the PIM notified if a directly connected source arrives. This procedure is how PIM sends register messages for new sources.

Examples

The following is sample output from the **show ipv6 mrib route** command using the **summary** keyword:

```
Device# show ipv6 mrib route summary
MRIB Route-DB Summary
  No. of (*,G) routes = 52
  No. of (S,G) routes = 0
  No. of Route x Interfaces (RxI) = 10
```

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

Table 40: 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-address source-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 Everest 16.6.1		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:

```
Device# show ipv6 mroute ff07::1
Multicast Routing Table
Flags:D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
      C - Connected, L - Local, I - Received Source Specific Host Report,
      P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
      J - Join SPT
Timers:Uptime/Expires
Interface state:Interface, State
(*, FF07::1), 00:04:45/00:02:47, RP 2001:0DB8:6::6, flags:S
  Incoming interface: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:

```
Device# show ipv6 mroute ff07::1 summary
Multicast Routing Table
Flags:D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
      C - Connected, L - Local, I - Received Source Specific Host Report,
      P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
      J - Join SPT
Timers:Uptime/Expires
Interface state:Interface, State
```

show ipv6 mroute

```
(*, 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:

```
Device# show ipv6 mroute ff07::1 count
IP Multicast Statistics
71 routes, 24 groups, 0.04 average sources per group
Forwarding Counts:Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
Other counts:Total/RPF failed/Other drops(OIF-null, rate-limit etc)
Group:FF07::1
RP-tree:
  RP Forwarding:0/0/0/0, Other:0/0/0
  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 41: show ipv6 mroute Field Descriptions

Field	Description
Flags:	<p>Provides information about the entry.</p> <ul style="list-style-type: none"> • 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:	<p>Indicates the state of the incoming or outgoing interface.</p> <ul style="list-style-type: none"> • 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.

show ipv6 mtu

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 Everest 16.6.1	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:

```
Device# show ipv6 mtu
MTU      Since      Destination Address
1400    00:04:21   5000:1::3
1280    00:04:50   FE80::203:A0FF:FED6:141D
```

The following is sample output from the **show ipv6 mtu** command using the **vrf** keyword and *vrfname* argument. This example provides information about the VRF named *vrfname1*:

```
Device# show ipv6 mtu vrf vrfname1
MTU      Since      Source Address      Destination Address
1300    00:00:04   2001:0DB8:2        2001:0DB8:7
```

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

Table 42: 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 <i>vrf-name</i>	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
<i>interface-type</i>	(Optional) Specifies the Interface type.
<i>interface-number</i>	(Optional) Specifies the Interface number.

Command Modes

User EXEC (>)

Privileged EXEC (#)

show ipv6 nd on-link prefix

Command History

Release	Modification
Cisco IOS XE Everest 16.6.1	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

```
Device# show ipv6 nd destination

IPv6 ND destination cache (table: default)
Code: R - Redirect
2001::1 [8]
    via FE80::A8BB:CCFF:FE00:5B00/Ethernet0/0
```

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

Table 43: 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 Everest 16.6.1	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-name** keyword and argument pair is used, then only information about the specified VRF is displayed. If the **interface-type** and **interface-number** arguments are used, then only information about the specified interface is displayed.

Examples

The following example displays information about on-link prefixes learned through RAs:

```
Device# show ipv6 nd on-link prefix
IPv6 ND on-link Prefix (table: default), 2 prefixes
Code: A - Autonomous Address Config
A 2001::/64 [2591994/604794]
router FE80::A8BB:CCFF:FE00:5A00/Ethernet0/0
2001:1:2::/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-number} {ipv6-address} {ipv6-hostname} | **statistics]**

Syntax Description	
<i>interface-type</i>	(Optional) Specifies the type of the interface from which IPv6 neighbor information is to be displayed.
<i>interface-number</i>	(Optional) Specifies the number of the interface from which IPv6 neighbor information is to be displayed.
<i>ipv6-address</i>	(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.
<i>ipv6-hostname</i>	(Optional) Specifies the IPv6 hostname of the remote networking device.
statistics	(Optional) Displays ND cache statistics.

show ipv6 neighbors

Command Default All IPv6 ND cache entries are listed.

Command Modes User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Everest 16.6.1	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:

```
Device# 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:

```
Device# 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 44: 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.

Field	Description
State	<p>The state of the neighbor cache entry. Following are the states for dynamic entries in the IPv6 neighbor discovery cache:</p> <ul style="list-style-type: none"> • 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. <p>Following are the possible states for static entries in the IPv6 neighbor discovery cache:</p> <ul style="list-style-type: none"> • INCMP (Incomplete)--The interface for this entry is down. • REACH (Reachable)--The interface for this entry is up. <p>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.</p>
Interface	Interface from which the address was reachable.

The following is sample output from the **show ipv6 neighbors** command with the **statistics** keyword:

```
Device# show ipv6 neighbor statistics

IPv6 ND Statistics
Entries 2, High-water 2, Gleaned 1, Scavenged 0
Entry States
    INCMP 0  REACH 0  STALE 2  GLEAN 0  DELAY 0  PROBE 0
Resolutions (INCMP)
    Requested 1, timeouts 0, resolved 1, failed 0
    In-progress 0, High-water 1, Throttled 0, Data discards 0
Resolutions (PROBE)
    Requested 3, timeouts 0, resolved 3, failed 0
```

The table below describes the significant fields shown in this display:

show ipv6 nhrp

Table 45: 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: <ul style="list-style-type: none"> • 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.
Resolutions (PROBE)	Statistics for neighbor resolutions attempted in PROBE state (that is, re-resolutions of existing entries prompted by a data packet): <ul style="list-style-type: none"> • Requested--Total number of resolutions requested. • Timeouts--Number of timeouts during resolutions. • Resolved--Number of successful resolutions. • Failed--Number of unsuccessful resolutions.

show ipv6 nhrp

To display Next Hop Resolution Protocol (NHRP) mapping information, use the **show ipv6 nhrp** command in user EXEC or privileged EXEC mode.

show ipv6 nhrp [{dynamic [*ipv6-address*] | incomplete | static}] [{address | interface}] [{brief | detail}] [purge]

Syntax Description	dynamic	(Optional) Displays dynamic (learned) IPv6-to-nonbroadcast multiaccess address (NBMA) mapping entries. Dynamic NHRP mapping entries are obtained from NHRP resolution/registration exchanges. See the table below for types, number ranges, and descriptions.
	<i>ipv6-address</i>	(Optional) The IPv6 address of the cache entry.
	incomplete	(Optional) Displays information about NHRP mapping entries for which the IPv6-to-NBMA is not resolved. See the table below for types, number ranges, and descriptions.
	static	(Optional) Displays static IPv6-to-NBMA address mapping entries. Static NHRP mapping entries are configured using the ipv6 nhrp map command. See the table below for types, number ranges, and descriptions.
	<i>address</i>	(Optional) NHRP mapping entry for specified protocol addresses.
	<i>interface</i>	(Optional) NHRP mapping entry for the specified interface. See the table below for types, number ranges, and descriptions.
	brief	(Optional) Displays a short output of the NHRP mapping.
	detail	(Optional) Displays detailed information about NHRP mapping.
	purge	(Optional) Displays NHRP purge information.

Command Modes User EXEC (>)

Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines The table below lists the valid types, number ranges, and descriptions for the optional *interface* argument.



Note The valid types can vary according to the platform and interfaces on the platform.

Table 46: Valid Types, Number Ranges, and Interface Description

Valid Types	Number Ranges	Interface Descriptions
async	1	Async
atm	0 to 6	ATM
bvi	1 to 255	Bridge-Group Virtual Interface

show ipv6 nhrp

Valid Types	Number Ranges	Interface Descriptions
cdma-ix	1	CDMA Ix
ctunnel	0 to 2147483647	C-Tunnel
dialer	0 to 20049	Dialer
ethernet	0 to 4294967295	Ethernet
fastethernet	0 to 6	FastEthernet IEEE 802.3
lex	0 to 2147483647	Lex
loopback	0 to 2147483647	Loopback
mfr	0 to 2147483647	Multilink Frame Relay bundle
multilink	0 to 2147483647	Multilink-group
null	0	Null
port-channel	1 to 64	Port channel
tunnel	0 to 2147483647	Tunnel
vif	1	PGM multicast host
virtual-ppp	0 to 2147483647	Virtual PPP
virtual-template	1 to 1000	Virtual template
virtual-tokenring	0 to 2147483647	Virtual Token Ring
xtagatm	0 to 2147483647	Extended tag ATM

Examples

The following is sample output from the **show ipv6 nhrp** command:

```
Device# show ipv6 nhrp
2001:0db8:3c4d:0015::1a2f:3d2c/48 via
2001:0db8:3c4d:0015::1a2f:3d2c
Tunnel0 created 6d05h, never expire
```

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

Table 47: show ipv6 nhrp Field Descriptions

Field	Description
2001:0db8:3c4d:0015::1a2f:3d2c/48	Target network.
2001:0db8:3c4d:0015::1a2f:3d2c	Next hop to reach the target network.
Tunnel0	Interface through which the target network is reached.

Field	Description
created 6d05h	Length of time since the entry was created (dayshours).
never expire	Indicates that static entries never expire.

The following is sample output from the **show ipv6 nhrp** command using the **brief** keyword:

```
Device# show ipv6 nhrp brief
2001:0db8:3c4d:0015:0000:0000:1a2f:3d2c/48
  via 2001:0db8:3c4d:0015:0000:0000:1a2f:3d2c
Interface: Tunnel0 Type: static
NBMA address: 10.11.11.99
```

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

Table 48: show ipv6 nhrp brief Field Descriptions

Field	Description
2001:0db8:3c4d:0015:0000:0000:1a2f:3d2c/48	Target network.
via 2001:0db8:3c4d:0015:0000:0000:1a2f:3d2c	Next Hop to reach the target network.
Interface: Tunnel0	Interface through which the target network is reached.
Type: static	Type of tunnel. The types can be one of the following: <ul style="list-style-type: none"> dynamic--NHRP mapping is obtained dynamically. The mapping entry is created using information from the NHRP resolution and registrations. static--NHRP mapping is configured statically. Entries configured by the ipv6 nhrp map command are marked static. incomplete--The NBMA address is not known for the target network.

Related Commands	Command	Description
	ipv6 nhrp map	Statically configures the IPv6-to-NBMA address mapping of IP destinations connected to an NBMA network.

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

show ipv6 ospf [process-id] [area-id] [rate-limit]

Syntax Description	<p>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.</p> <p>area-id (Optional) Area ID. This argument displays information about a specified area only.</p> <p>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.</p>
---------------------------	---

Command Modes User EXEC (>)

Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

show ipv6 ospf Output Example

The following is sample output from the **show ipv6 ospf** command:

```
Device# show ipv6 ospf
Routing Process "ospfv3 1" with ID 10.10.10.1
  SPF schedule delay 5 secs, Hold time between two 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 49: 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).

Field	Description
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:

```
Device# show ipv6 ospf
Routing Process "ospfv3 1" with ID 10.0.0.1
It is an area border device
SPF schedule delay 5 secs, Hold time between two 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 50: show ipv6 ospf with Area Encryption Information Field Descriptions

Field	Description
Area 1	Subsequent fields describe area 1.
NULL Encryption SHA-1 Auth, SPI 1001	Displays the encryption algorithm (in this case, null, meaning no encryption algorithm is used), the authentication algorithm (SHA-1), and the security policy index (SPI) value (1001).

The following example displays the configuration values for SPF and LSA throttling timers:

```
Device# show ipv6 ospf
Routing Process "ospfv3 1" with ID 10.9.4.1
Event-log enabled, Maximum number of events: 1000, Mode: cyclic
```

show ipv6 ospf

```

It is an autonomous system boundary device
Redistributing External Routes from,
    ospf 2
Initial SPF schedule delay 5000 msec
Minimum hold time between two consecutive SPFs 10000 msec
Maximum wait time between two consecutive SPFs 10000 msec
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msec

```

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

Table 51: 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 msec	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 msec	Maximum arrival time (in milliseconds) of link-state advertisements.

The following example shows information about LSAs that are currently being rate limited:

```

Device# show ipv6 ospf rate-limit
List of LSAs that are in rate limit Queue
    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 52: show ipv6 ospf rate-limit Field Descriptions

Field	Description
LSAID	Link-state ID of the LSA.
Type	Description of the LSA.
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	<i>process-id</i> (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 Everest 16.6.1	This command was introduced.

Examples

The following is sample output from the **show ipv6 ospf border-routers** command:

```
Device# show ipv6 ospf border-routers

OSPFv3 Process 1 internal Routing Table
Codes: i - Intra-area route, I - Inter-area route
i 172.16.4.4 [2] via FE80::205:5FFF:FED3:5808, FastEthernet0/0, ABR, Area 1, SPF 13
i 172.16.4.4 [1] via FE80::205:5FFF:FED3:5406, POS4/0, ABR, Area 0, SPF 8
i 172.16.3.3 [1] via FE80::205:5FFF:FED3:5808, FastEthernet0/0, ASBR, Area 1, SPF 3
```

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

Table 53: 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.

show ipv6 ospf event

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 (#)

Release	Modification
Cisco IOS XE Everest 16.6.1	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:

```

Device# show ipv6 ospf event spf lsa reverse

OSPFv3 Router with ID (10.0.0.1) (Process ID 1)
1 *Sep 29 11:59:18.367: Rcv Changed Type-0x2009 LSA, LSID 10.0.0.0, Adv-Rtr 192.168.0.1,
Seq# 80007699, Age 3600
3 *Sep 29 11:59:18.367: Schedule SPF, Area 0, Change in LSID 10.0.0.0, LSA type P
4 *Sep 29 11:59:18.367: Rcv Changed Type-0x2001 LSA, LSID 10.0.0.0, Adv-Rtr 192.168.0.1,
Seq# 80007699, Age 2
5 *Sep 29 11:59:18.367: Schedule SPF, Area 0, Change in LSID 10.0.0.0, LSA type R
6 *Sep 29 11:59:18.367: Rcv Changed Type-0x2002 LSA, LSID 10.1.0.1, Adv-Rtr 192.168.0.1,
Seq# 80007699, Age 3600
8 *Sep 29 11:59:18.367: Schedule SPF, Area 0, Change in LSID 10.1.0.1, LSA type N
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 54: 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).

show ipv6 ospf graceful-restart

Field	Description
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 Everest 16.6.1		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:

```
Device# show ipv6 ospf graceful-restart
Routing Process "ospf 1"
Graceful Restart enabled
  restart-interval limit: 120 sec, last restart 00:00:15 ago (took 36 secs)
  Graceful Restart helper support enabled
  Router status : Active
  Router is running in SSO mode
  OSPF restart state : NO_RESTART
  Router ID 10.1.1.1, checkpoint Router ID 10.0.0.0
```

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

Table 55: 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.
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 **show ipv6 ospf interface** command in user EXEC or privileged mode.

show ipv6 ospf [process-id] [area-id] interface [type number] [brief]

Syntax Description	<i>process-id</i>	(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.
	<i>area-id</i>	(Optional) Displays information about a specified area only.
	<i>type number</i>	(Optional) Interface type and number.
	brief	(Optional) Displays brief overview information for OSPF interfaces, states, addresses and masks, and areas on the router.

show ipv6 ospf interface**Command Modes** User EXEC (>)

Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Examples**show ipv6 ospf interface Standard Output Example**

The following is sample output from the **show ipv6 ospf interface** command:

```
Device# show ipv6 ospf interface
ATM3/0 is up, line protocol is up
  Link Local Address 2001:0DB1:205:5FFF:FED3:5808, Interface ID 13
  Area 1, Process ID 1, Instance ID 0, Router ID 172.16.3.3
  Network Type POINT_TO_POINT, Cost: 1
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
  Index 1/2/2, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 12, maximum is 12
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 172.16.4.4
    Suppress hello for 0 neighbor(s)
FastEthernet0/0 is up, line protocol is up
  Link Local Address 2001:0DB1:205:5FFF:FED3:5808, Interface ID 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 56: 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.

Field	Description
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.

```
Device# show ipv6 ospf interface brief
```

Interface	PID	Area	Intf	ID	Cost	State	Nbrs	F/C
VLO	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:

```
Device# show ipv6 ospf interface
Ethernet0/0 is up, line protocol is up
  Link Local Address 2001:0DB1:A8BB:CCFF:FE00:6E00, Interface ID 2
  Area 0, Process ID 1, Instance ID 0, Router ID 10.10.10.1
  Network Type BROADCAST, Cost:10
  MD5 Authentication SPI 500, secure socket state UP (errors:0)
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 10.11.11.1, local address 2001:0DB1:A8BB:CCFF:FE00:6F00
  Backup Designated router (ID) 10.10.10.1, local address
  2001:0DB1:A8BB:CCFF:FE00:6E00
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:01
  Index 1/1/1, flood queue length 0
  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)
```

show ipv6 ospf interface

OSPF with Null Authentication Example

The following is sample output from the **show ipv6 ospf interface** command with null authentication configured on the interface:

```
Device# show ipv6 ospf interface
Ethernet0/0 is up, line protocol is up
  Link Local Address 2001:0DB1:A8BB:CCFF:FE00:6E00, Interface ID 2
  Area 0, Process ID 1, Instance ID 0, Router ID 10.10.10.1
  Network Type BROADCAST, Cost:10
  Authentication NULL
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 10.11.11.1, local address 2001:0DB1:A8BB:CCFF:FE00:6F00
  Backup Designated router (ID) 10.10.10.1, local address
  2001:0DB1:A8BB:CCFF:FE00:6E00
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:03
  Index 1/1/1, flood queue length 0
  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 **show ipv6 ospf interface** command with authentication configured for the area:

```
Device# show ipv6 ospf interface
Ethernet0/0 is up, line protocol is up
  Link Local Address 2001:0DB1:A8BB:CCFF:FE00:6E00, Interface ID 2
  Area 0, Process ID 1, Instance ID 0, Router ID 10.10.10.1
  Network Type BROADCAST, Cost:10
  MD5 Authentication (Area) SPI 1000, secure socket state UP (errors:0)
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 10.11.11.1, local address 2001:0DB1:A8BB:CCFF:FE00:6F00
  Backup Designated router (ID) 10.10.10.1, local address
  FE80::A8BB:CCFF:FE00:6E00
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:03
  Index 1/1/1, flood queue length 0
  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 **show ipv6 ospf interface** command when the OSPF cost dynamic is configured.

```
Device# show ipv6 ospf interface serial 2/0
```

```

Serial2/0 is up, line protocol is up
  Link Local Address 2001:0DB1:A8BB:CCFF:FE00:100, Interface ID 10
  Area 1, Process ID 1, Instance ID 0, Router ID 172.1.1.1
  Network Type POINT_TO_MULTIPOINT, Cost: 64 (dynamic), Cost Hysteresis: 200
  Cost Weights: Throughput 100, Resources 20, Latency 80, L2-factor 100
  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 **show ipv6 ospf interface** command when the OSPF graceful restart feature is configured:

```

Device# show ipv6 ospf interface
Ethernet0/0 is up, line protocol is up
  Link Local Address FE80::A8BB:CCFF:FE00:300, Interface ID 2
  Area 0, Process ID 1, Instance ID 0, Router ID 10.3.3.3
  Network Type POINT_TO_POINT, Cost: 10
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Graceful Restart p2p timeout in 00:00:19
    Hello due in 00:00:02
  Graceful Restart helper support enabled
  Index 1/1/1, flood queue length 0
  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):

```

Device# show ipv6 ospf interface
Serial10/0 is up, line protocol is up
  Link Local Address FE80::A8BB:CCFF:FE00:6500, Interface ID 42
  Area 1, Process ID 1, Instance ID 0, Router ID 10.0.0.1
  Network Type POINT_TO_POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT_TO_POINT, BFD enabled
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:07
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  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)

```

show ipv6 ospf request-list

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

<i>process-id</i>	(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.
<i>area-id</i>	(Optional) Displays information only about a specified area.
<i>neighbor</i>	(Optional) Displays the list of all LSAs requested by the router from this neighbor.
<i>interface</i>	(Optional) Displays the list of all LSAs requested by the router from this interface.
<i>interface-neighbor</i>	(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 Everest 16.6.1	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:

```
Device# show ipv6 ospf request-list

          OSPFv3 Router with ID (192.168.255.5) (Process ID 1)
          Neighbor 192.168.255.2, interface Ethernet0/0 address
          FE80::A8BB:CCFF:FE00:6600
          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 57: 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	<table border="1"> <tr> <td><i>process-id</i></td><td>(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when the OSPF routing process is enabled.</td></tr> <tr> <td><i>area-id</i></td><td>(Optional) Displays information only about a specified area.</td></tr> <tr> <td><i>neighbor</i></td><td>(Optional) Displays the list of all LSAs waiting to be re-sent for this neighbor.</td></tr> <tr> <td><i>interface</i></td><td>(Optional) Displays the list of all LSAs waiting to be re-sent on this interface.</td></tr> <tr> <td><i>interface neighbor</i></td><td>(Optional) Displays the list of all LSAs waiting to be re-sent on this interface, from this neighbor.</td></tr> </table>	<i>process-id</i>	(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.	<i>area-id</i>	(Optional) Displays information only about a specified area.	<i>neighbor</i>	(Optional) Displays the list of all LSAs waiting to be re-sent for this neighbor.	<i>interface</i>	(Optional) Displays the list of all LSAs waiting to be re-sent on this interface.	<i>interface neighbor</i>	(Optional) Displays the list of all LSAs waiting to be re-sent on this interface, from this neighbor.
<i>process-id</i>	(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.										
<i>area-id</i>	(Optional) Displays information only about a specified area.										
<i>neighbor</i>	(Optional) Displays the list of all LSAs waiting to be re-sent for this neighbor.										
<i>interface</i>	(Optional) Displays the list of all LSAs waiting to be re-sent on this interface.										
<i>interface neighbor</i>	(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 Everest 16.6.1	This command was introduced.

show ipv6 ospf statistics**Usage Guidelines**

The information displayed by the **show ipv6 ospf retransmission-list** command is useful in debugging Open Shortest Path First (OSPF) routing operations.

Examples

The following is sample output from the **show ipv6 ospf retransmission-list** command:

```
Device# show ipv6 ospf retransmission-list

    OSPFv3 Router with ID (192.168.255.2) (Process ID 1)
    Neighbor 192.168.255.1, interface Ethernet0/0
    Link state retransmission due in 3759 msec, Queue length 1
    Type      LS ID          ADV RTR        Seq NO     Age      Checksum
    0x2001   0              192.168.255.2  0x80000222  1        0x00AE52
```

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

Table 58: 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.
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 Everest 16.6.1	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:

```
Device# show ipv6 ospf statistics detail
  Area 0: SPF algorithm executed 3 times
  SPF 1 executed 00:06:57 ago, SPF type Full
    SPF calculation time (in msec):
      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 59: 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.

show ipv6 ospf summary-prefix

Field	Description
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: <ul style="list-style-type: none"> • 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	<i>process-id</i> (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	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	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:

```
Device# show ipv6 ospf summary-prefix
```

```
OSPFv3 Process 1, Summary-prefix
FEC0::/24 Metric 16777215, Type 0, Tag 0
```

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

Table 60: 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 Everest 16.6.1		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:

```
Device# show ipv6 ospf timers rate-limit
List of LSAs that are in rate limit Queue
    LSAID: 0.0.0.0 Type: 0x2001 Adv Rtr: 55.55.55.55 Due in: 00:00:00.500
    LSAID: 0.0.0.0 Type: 0x2009 Adv Rtr: 55.55.55.55 Due in: 00:00:00.500
```

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

show ipv6 ospf traffic

Table 61: 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	<table border="1"> <tr> <td><i>process-id</i></td><td>(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).</td></tr> <tr> <td><i>interface-type interface-number</i></td><td>(Optional) Type and number associated with a specific OSPF interface.</td></tr> </table>	<i>process-id</i>	(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).	<i>interface-type interface-number</i>	(Optional) Type and number associated with a specific OSPF interface.
<i>process-id</i>	(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).				
<i>interface-type interface-number</i>	(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 Everest 16.6.1	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 <i>process-id</i> argument, or you can limit output to traffic statistics for a specific interface associated with an OSPF process by entering values for the <i>interface-type</i> and <i>interface-number</i> arguments. To reset counters and clear statistics, use the clear ipv6 ospf traffic command.
-------------------------	--

Examples	The following example shows the display output for the show ipv6 ospf traffic command for OSPFv3:
-----------------	--

```
Device# show ipv6 ospf traffic
OSPFv3 statistics:
Rcvd: 32 total, 0 checksum errors
    10 hello, 7 database desc, 2 link state req
    9 link state updates, 4 link state acks
```

```

    0 LSA ignored
Sent: 45 total, 0 failed
    17 hello, 12 database desc, 2 link state req
    8 link state updates, 6 link state acks
    OSPFv3 Router with ID (10.1.1.4) (Process ID 6)
OSPFv3 queues statistic for process ID 6
    Hello queue size 0, no limit, max size 2
    Router queue size 0, limit 200, drops 0, max size 2
Interface statistics:
    Interface Serial2/0
OSPFv3 packets received/sent
    Type      Packets      Bytes
    RX Invalid  0          0
    RX Hello   5          196
    RX DB des  4          172
    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

```

show ipv6 ospf traffic

```

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:

```
Device# clear ipv6 ospf traffic
```

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

Table 62: 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.

Field	Description
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	<p>Summary traffic statistics accumulated for an OSPFv3 process.</p> <p>Note The OSPF process ID is a unique value assigned to the OSPFv3 process in the configuration.</p> <p>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.</p>

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 **show 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 Everest 16.6.1	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:

```
Device# show ipv6 ospf virtual-links
Virtual Link OSPF_VL0 to router 172.16.6.6 is up
  Interface ID 27, IPv6 address FEC0:6666:6666::
```

Run as demand circuit

show ipv6 ospf virtual-links

```

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 63: 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.
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.

```

Device# show ipv6 ospf virtual-links
Virtual Link OSPFv3_VL1 to router 10.2.0.1 is up
  Interface ID 69, IPv6 address 2001:0DB8:11:0:A8BB:CCFF:FE00:6A00
  Run as demand circuit
  DoNotAge LSA allowed.
  Transit area 1, via interface Serial12/0, Cost of using 64
  NULL encryption SHA-1 auth SPI 3944, secure socket UP (errors: 0)
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 2, Dead 10, Wait 40, Retransmit 5
    Adjacency State FULL (Hello suppressed)
    Index 1/2/4, retransmission queue length 0, number of retransmission 1
    First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
    Last retransmission scan length is 1, maximum is 1
    Last retransmission scan time is 0 msec, maximum is 0 msec
Virtual Link OSPFv3_VL0 to router 10.1.0.1 is up
  Interface ID 67, IPv6 address 2001:0DB8:13:0:A8BB:CCFF:FE00:6700
  Run as demand circuit
  DoNotAge LSA allowed.
  Transit area 1, via interface Serial11/0, Cost of using 128
  MD5 authentication SPI 940, secure socket UP (errors: 0)
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Adjacency State FULL (Hello suppressed)
    Index 1/1/3, retransmission queue length 0, number of retransmission 1
    First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)

```

```
Last retransmission scan length is 1, maximum is 1
Last retransmission scan time is 0 msec, maximum is 0 msec
```

show ipv6 pim anycast-RP

To verify IPv6 PIM anycast RP operation, use the **show ipv6 pim anycast-RP** command in user EXEC or privileged EXEC mode.

show ipv6 pim anycast-RP *rp-address*

Syntax Description	<i>rp-address</i> RP address to be verified.
---------------------------	--

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

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines

Examples Device# **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 <i>vrf-name</i> (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.

show ipv6 pim 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 Everest 16.6.1	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:

```
Device# show ipv6 pim bsr election
PIMv2 BSR information
BSR Election Information
Scope Range List: ff00::/8
This system is the Bootstrap Router (BSR)
BSR Address: 60::1:1:4
Uptime: 00:11:55, BSR Priority: 0, Hash mask length: 126
RPF: FE80::A8BB:CCFF:FE03:C400, Ethernet0/0
BS Timer: 00:00:07
This system is candidate BSR
Candidate BSR address: 60::1:1:4, priority: 0, hash mask length: 126
```

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

Table 64: show ipv6 pim bsr election Field Descriptions

Field	Description
Scope Range List	Scope to which this BSR information applies.
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:

```
Device# show ipv6 pim bsr rp-cache
PIMv2 BSR C-RP Cache
BSR Candidate RP Cache
Group(s) FF00::/8, RP count 2
  RP 10::1:1:3
    Priority 192, Holdtime 150
    Uptime: 00:12:36, expires: 00:01:55
  RP 20::1:1:1
    Priority 192, Holdtime 150
    Uptime: 00:12:36, expires: 00:01:5
```

The following example displays information about the C-RP. This RP has been configured without a specific scope value, so the RP will send C-RP advertisements to all BSRs about which it has learned through BSMs it has received.

```
Device# show ipv6 pim bsr candidate-rp
PIMv2 C-RP information
  Candidate RP: 10::1:1:3
    All Learnt Scoped Zones, Priority 192, Holdtime 150
    Advertisement interval 60 seconds
    Next advertisement in 00:00:33
```

The following example confirms that the IPv6 C-BSR is PIM-enabled. If PIM is disabled on an IPv6 C-BSR interface, or if a C-BSR or C-RP is configured with the address of an interface that does not have PIM enabled, the **show ipv6 pim bsr** command used with the **election** keyword would display that information instead.

```
Device# show ipv6 pim bsr election
PIMv2 BSR information

BSR Election Information
Scope Range List: ff00::/8
  BSR Address: 2001:DB8:1:1:2
  Uptime: 00:02:42, BSR Priority: 34, Hash mask length: 28
  RPF: FE80::20:1:2, Ethernet1/0
  BS Timer: 00:01:27
```

show ipv6 pim df

To display the designated forwarder (DF)-election state of each interface for each rendezvous point (RP), use the **show ipv6 pim df** command in user EXEC or privileged EXEC mode.

show ipv6 pim [vrf vrf-name] df [interface-type interface-number] [rp-address]

Syntax Description	vrf vrf-name	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
	<i>interface-type interface-number</i>	(Optional) Interface type and number. For more information, use the question mark (?) online help function.
	<i>rp-address</i>	(Optional) RP IPv6 address.

Command Default If no interface or RP address is specified, all DFs are displayed.

show ipv6 pim df

Command Modes	User EXEC (>) Privileged EXEC (#)										
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.						
Release	Modification										
Cisco IOS XE Everest 16.6.1	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	<p>The following example displays the DF-election states:</p> <pre>Device# show ipv6 pim df Interface DF State Timer Metrics Ethernet0/0 Winner 4s 8ms [120/2] RP :200::1 Ethernet1/0 Lose 0s 0ms [inf/inf] RP :200::1</pre> <p>The following example shows information on the RP:</p> <pre>Device# show ipv6 pim df Interface DF State Timer Metrics Ethernet0/0 None:RP LAN 0s 0ms [inf/inf] RP :200::1 Ethernet1/0 Winner 7s 600ms [0/0] RP :200::1 Ethernet2/0 Winner 9s 8ms [0/0] RP :200::1</pre>										
	<p>The table below describes the significant fields shown in the display.</p> <p>Table 65: show ipv6 pim df Field Descriptions</p> <table border="1"> <thead> <tr> <th>Field</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Interface</td> <td>Interface type and number that is configured to run PIM.</td> </tr> <tr> <td>DF State</td> <td> <p>The state of the DF election on the interface. The state can be:</p> <ul style="list-style-type: none"> • Offer • Winner • Backoff • Lose • None:RP LAN <p>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.</p> </td> </tr> <tr> <td>Timer</td> <td>DF election timer.</td> </tr> <tr> <td>Metrics</td> <td>Routing metrics to the RP announced by the DF.</td> </tr> </tbody> </table>	Field	Description	Interface	Interface type and number that is configured to run PIM.	DF State	<p>The state of the DF election on the interface. The state can be:</p> <ul style="list-style-type: none"> • Offer • Winner • Backoff • Lose • None:RP LAN <p>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.</p>	Timer	DF election timer.	Metrics	Routing metrics to the RP announced by the DF.
Field	Description										
Interface	Interface type and number that is configured to run PIM.										
DF State	<p>The state of the DF election on the interface. The state can be:</p> <ul style="list-style-type: none"> • Offer • Winner • Backoff • Lose • None:RP LAN <p>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.</p>										
Timer	DF election timer.										
Metrics	Routing metrics to the RP announced by the DF.										

Field	Description
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-name|group-address}]|[{group-range|group-mask}] [info-source {bsr | default | embedded-rp | static}]}}
```

Syntax Description	vrf vrf-name	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
	<i>group-name</i> <i>group-address</i>	(Optional) IPv6 address or name of the multicast group.
	<i>group-range</i> <i>group-mask</i>	(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 Everest 16.6.1	This command was introduced.

show ipv6 pim group-map

Usage Guidelines

Use the **show ipv6 pim group-map** command to find all group mappings installed by a given source of information, such as BSR or static configuration.

You can also use this command to find which group mapping a router at a specified IPv6 group address is using by specifying a group address, or to find an exact group mapping entry by specifying a group range and mask length.

Examples

The following is sample output from the **show ipv6 pim group-map** command:

```
Device# show ipv6 pim group-map
FF33::/32*
    SSM
    Info source:Static
    Uptime:00:08:32, Groups:0
FF34::/32*
    SSM
    Info source:Static
    Uptime:00:09:42, Groups:0
```

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

Table 66: 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	<table border="1"> <tr> <td>vrf vrf-name</td><td>(Optional) Specifies a virtual routing and forwarding (VRF) configuration.</td></tr> <tr> <td>state-on</td><td>(Optional) Displays interfaces with PIM enabled.</td></tr> <tr> <td>state-off</td><td>(Optional) Displays interfaces with PIM disabled.</td></tr> <tr> <td>type number</td><td>(Optional) Interface type and number.</td></tr> </table>	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.
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
		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:

```
Device# 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.

show ipv6 pim join-prune statistic

Table 67: 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:

```
Device(config)# show ipv6 pim interface gigabitethernet0/0/0

      Interface          PIM     Nbr     Hello    DR    BFD
                  Count   Intvl Prior

      GigabitEthernet0/0/0    on/P   0       30      1    On
      Address: FE80::A8BB:CCFF:FE00:9100
      DR       : this system
```

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

Table 68: 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.
---------------------	--

<i>interface-type</i>	(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 Everest 16.6.1		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:

```
Device# show ipv6 pim join-prune statistic Ethernet0/0/0
PIM Average Join/Prune Aggregation for last (1K/10K/50K) packets
Interface          Transmitted          Received
Ethernet0/0/0      0 / 0 / 0           1 / 0 / 0
```

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

Table 69: 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	<i>vrf vrf-name</i>	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
	<i>interface</i>	(Optional) Specific interface for which limit information is provided.

Command Modes Privileged EXEC (#)

show ipv6 pim neighbor

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines	The show ipv6 pim limit command checks interface statistics for limits. If the optional <i>interface</i> argument is enabled, only information for the specified interface is shown.
Examples	The following example displays PIM interface limit information:


```
Device# show ipv6 pim limit
```

Related Commands	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 <i>vrf-name</i>	(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.
	<i>interface-type interface-number</i>	(Optional) Interface type and number.
	count	(Optional) Displays neighbor counts on each interface.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	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:

```
Device# show ipv6 pim neighbor detail

Neighbor Address(es)           Interface          Uptime   Expires DR pri Bidir
FE80::A8BB:CCFF:FE00:401      Ethernet0/0        01:34:16 00:01:16 1      B
60::1:1:3

FE80::A8BB:CCFF:FE00:501      Ethernet0/0        01:34:15 00:01:18 1      B
60::1:1:4
```

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

Table 70: 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.
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 (#)

show ipv6 pim topology

Command History

Release	Modification
Cisco IOS XE Everest 16.6.1	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:

```
Device# show ipv6 pim range-list
config SSM Exp:never Learnt from :::
FF33::/32 Up:00:26:33
FF34::/32 Up:00:26:33
FF35::/32 Up:00:26:33
FF36::/32 Up:00:26:33
FF37::/32 Up:00:26:33
FF38::/32 Up:00:26:33
FF39::/32 Up:00:26:33
FF3A::/32 Up:00:26:33
FF3B::/32 Up:00:26:33
FF3C::/32 Up:00:26:33
FF3D::/32 Up:00:26:33
FF3E::/32 Up:00:26:33
FF3F::/32 Up:00:26:33
config SM RP:40::1:1:1 Exp:never Learnt from :::
FF13::/64 Up:00:03:50
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 71: 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-address|source-name}] | link-local} ]route-count [detail]
```

Syntax Description	vrf <i>vrf-name</i>	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
	<i>group-name</i> <i>group-address</i>	(Optional) IPv6 address or name of the multicast group.
	<i>source-address</i> <i>source-name</i>	(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 Everest 16.6.1		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:

```
Device# 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
```

show ipv6 pim traffic

```

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 72: 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 Everest 16.6.1	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.

```
Device# show ipv6 pim traffic

PIM Traffic Counters
Elapsed time since counters cleared:00:05:29
          Received    Sent
Valid PIM Packets      22      22
Hello                  22      22
Join-Prune              0       0
Register                0       0
Register Stop            0       0
Assert                 0       0
Bidir DF Election       0       0
Errors:
Malformed Packets      0
Bad Checksums           0
Send Errors             0
Packet Sent on Loopback Errors 0
Packets Received on PIM-disabled Interface 0
Packets Received with Unknown PIM Version 0
```

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

Table 73: 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.
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

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.
	<i>interface-type interface-number</i>	(Optional) Tunnel interface type and number.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	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:

```
Device# show ipv6 pim tunnel
Tunnel0*
  Type    :PIM Encap
  RP      :100::1
  Source:100::1
Tunnel0*
  Type    :PIM Decap
  RP      :100::1
  Source: -
```

The following is sample output from the **show ipv6 pim tunnel** command on a non-RP:

```
Device# show ipv6 pim tunnel
Tunnel0*
  Type    :PIM Encap
  RP      :100::1
  Source:2001::1:1:1
```

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

Table 74: 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 Everest 16.6.1	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:

```
Device# 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

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	<table border="1"> <tr> <td>detail summary</td><td>(Optional) Displays detailed or summarized information about all IPv6 prefix lists.</td></tr> <tr> <td><i>list-name</i></td><td>(Optional) The name of a specific IPv6 prefix list.</td></tr> <tr> <td><i>ipv6-prefix</i></td><td>All prefix list entries for the specified IPv6 network. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.</td></tr> <tr> <td><i>/ prefix-length</i></td><td>The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.</td></tr> <tr> <td>longer</td><td>(Optional) Displays all entries of an IPv6 prefix list that are more specific than the given <i>ipv6-prefix / prefix-length</i> values.</td></tr> <tr> <td>first-match</td><td>(Optional) Displays the entry of an IPv6 prefix list that matches the given <i>ipv6-prefix / prefix-length</i> values.</td></tr> <tr> <td>seq seq-num</td><td>The sequence number of the IPv6 prefix list entry.</td></tr> </table>	detail summary	(Optional) Displays detailed or summarized information about all IPv6 prefix lists.	<i>list-name</i>	(Optional) The name of a specific IPv6 prefix list.	<i>ipv6-prefix</i>	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.	<i>/ prefix-length</i>	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 <i>ipv6-prefix / prefix-length</i> values.	first-match	(Optional) Displays the entry of an IPv6 prefix list that matches the given <i>ipv6-prefix / prefix-length</i> values.	seq seq-num	The sequence number of the IPv6 prefix list entry.
detail summary	(Optional) Displays detailed or summarized information about all IPv6 prefix lists.														
<i>list-name</i>	(Optional) The name of a specific IPv6 prefix list.														
<i>ipv6-prefix</i>	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.														
<i>/ prefix-length</i>	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 <i>ipv6-prefix / prefix-length</i> values.														
first-match	(Optional) Displays the entry of an IPv6 prefix list that matches the given <i>ipv6-prefix / prefix-length</i> 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 Everest 16.6.1	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:

```
Device# show ipv6 prefix-list detail
Prefix-list with the last deletion/insertion: bgp-in
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)
ipv6 prefix-list bgp-in:
  count: 6, range entries: 3, sequences: 5 - 30, refcount: 31
  seq 5 deny 5F00::/8 le 128 (hit count: 0, refcount: 1)
  seq 10 deny ::/0 (hit count: 0, refcount: 1)
  seq 15 deny ::/1 (hit count: 0, refcount: 1)
  seq 20 deny ::/2 (hit count: 0, refcount: 1)
  seq 25 deny ::/3 ge 4 (hit count: 0, refcount: 1)
  seq 30 permit ::/0 le 128 (hit count: 240664, refcount: 0)

```

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

Table 75: 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:

```

Device# show ipv6 prefix-list summary
Prefix-list with the last deletion/insertion: bgp-in
ipv6 prefix-list 6to4:
  count: 1, range entries: 0, sequences: 5 - 5, refcount: 2
  ipv6 prefix-list aggregate:
    count: 2, range entries: 2, sequences: 5 - 10, refcount: 30
  ipv6 prefix-list bgp-in:
    count: 6, range entries: 3, sequences: 5 - 30, refcount: 31

```

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.

show ipv6 protocols

Command	Description
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.
neighbor prefix-list	Distributes BGP neighbor information as specified in 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	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	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:

```
Device# show ipv6 protocols

IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "static"
IPv6 Routing Protocol is "isis"
  Interfaces:
    Ethernet0/0/3
    Ethernet0/0/1
    Serial11/0/1
    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 76: 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.

The following sample output from the **show ipv6 protocols** command displays the Border Gateway Protocol (BGP) information for autonomous system 30:

```
Device# show ipv6 protocols

IPv6 Routing Protocol is "bgp 30"
  IGP synchronization is disabled
  Redistribution:
    Redistributing protocol connected
  Neighbor(s):
    Address          FiltIn FiltOut Weight RoutemapIn RoutemapOut
    2001:DB8:0:ABCD::1      5       7     200
                                         rmap-in      rmap-out
    2001:DB8:0:ABCD::2
                                         rmap-in      rmap-out
    2001:DB8:0:ABCD::3
```

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

Table 77: show ipv6 protocols Field Descriptions for BGP Process

Field	Description
IPv6 Routing Protocol is	Specifies the IPv6 routing protocol used.
Redistribution	Lists the protocol that is being redistributed.
Address	Neighbor IPv6 address.
FiltIn	AS-path filter list applied to input.
FiltOut	AS-path filter list applied to output.
Weight	Neighbor weight value used in BGP best path selection.
RoutemapIn	Neighbor route map applied to input.

show ipv6 protocols

Field	Description
RoutemapOut	Neighbor route map applied to output.

The following is sample output from the **show ipv6 protocols summary** command:

```
Device# show ipv6 protocols summary

Index Process Name
0      connected
1      static
2      rip myrip
3      bgp 30
```

The following sample output from the **show ipv6 protocols** command displays the EIGRP information including the vector metric and EIGRP IPv6 NSF:

```
Device# show ipv6 protocols

IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "bgp 1"
  IGP synchronization is disabled
  Redistribution:
    None
IPv6 Routing Protocol is "bgp multicast"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "eigrp 1"
EIGRP-IPv6 VR(name) Address-Family Protocol for AS(1)
  Metric weight K1=1, K2=0, K3=1, K4=0, K5=0 K6=0
  Metric rib-scale 128
  Metric version 64bit
  NSF-aware route hold timer is 260
  EIGRP NSF enabled
    NSF signal timer is 15s
    NSF converge timer is 65s
  Router-ID: 10.1.2.2
  Topology : 0 (base)
    Active Timer: 3 min
    Distance: internal 90 external 170
    Maximum path: 16
    Maximum hopcount 100
    Maximum metric variance 1
    Total Prefix Count: 0
    Total Redist Count: 0

  Interfaces:
  Redistribution:
    None
```

The following example displays IPv6 protocol information after configuring redistribution in an Open Shortest Path First (OSPF) domain:

```
Device# redistribute ospf 1 match internal
Device(config-rtr) # end
Device# show ipv6 protocols

IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "rip 1"
  Interfaces:
```

```

Ethernet0/1
Loopback9
Redistribution:
  Redistributing protocol ospf 1 (internal)
  IPv6 Routing Protocol is "ospf 1"
  Interfaces (Area 0):
    Ethernet0/0
  Redistribution:
    None

```

show ipv6 rip

To display information about current IPv6 Routing Information Protocol (RIP) processes, use the **show ipv6 rip** command in user EXEC or privileged EXEC mode.

show ipv6 rip [name] [vrf vrf-name][{database | next-hops}]

show ipv6 rip [name] [{database | next-hops}]

Syntax Description	<table border="1"> <tr> <td>name</td><td>(Optional) Name of the RIP process. If the name is not entered, details of all configured RIP processes are displayed.</td></tr> <tr> <td>vrf vrf-name</td><td>(Optional) Displays information about the specified Virtual Routing and Forwarding (VRF) instance.</td></tr> <tr> <td>database</td><td>(Optional) Displays information about entries in the specified RIP IPv6 routing table.</td></tr> <tr> <td>next-hops</td><td>(Optional) Displays information about the next hop addresses for the specified RIP IPv6 process. If no RIP process name is specified, the next-hop addresses for all RIP IPv6 processes are displayed.</td></tr> </table>	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.
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 Everest 16.6.1	This command was introduced.

Examples The following is sample output from the **show ipv6 rip** command:

```

Device# show ipv6 rip

RIP process "one", port 521, multicast-group FF02::9, pid 55
  Administrative distance is 25. Maximum paths is 4
  Updates every 30 seconds, expire after 180
  Holddown lasts 0 seconds, garbage collect after 120
  Split horizon is on; poison reverse is off

```

show ipv6 rip

```

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 78: 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.

```
Device# show ipv6 rip one database
RIP process "one", local RIB
```

```

2001:72D:1000::/64, metric 2
    Ethernet2/2001:DB8:0:ABCD::1, expires in 168 secs
2001:72D:2000::/64, metric 2, installed
    Ethernet2/2001:DB8:0:ABCD::1, expires in 168 secs
2001:72D:3000::/64, metric 2, installed
    Ethernet2/2001:DB8:0:ABCD::1, expires in 168 secs
    Ethernet1/2001:DB8::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 79: 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.

```

Device# show ipv6 rip one next-hops

RIP process "one", Next Hops
    FE80::210:7BFF:FEC2:ACCF/Ethernet4/2 [1 routes]
    FE80::210:7BFF:FEC2:B286/Ethernet4/2 [2 routes]

```

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

Table 80: show ipv6 rip next-hops Field Descriptions

Field	Description
RIP process	The name of the RIP process.

show ipv6 rip

Field	Description
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:

```
Device# show ipv6 rip vrf red

RIP VRF "red", port 521, multicast-group 2001:DB8::/32, pid 295
Administrative distance is 120. Maximum paths is 16
Updates every 30 seconds, expire after 180
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 81: 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.

Field	Description
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 82: 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	<p>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.</p> <p>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.</p>
expires in	The interval (in seconds) before the route expires.

The following is sample output from **show ipv6 rip vrf database** command:

```
Device# show ipv6 rip vrf blue database
      RIP VRF "blue", Next Hops
      FE80::A8BB:CCFF:FE00:7C00/Ethernet0/0 [1 paths]
```

Table 83: 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.

show ipv6 route

Field	Description
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 route

To display contents of the IPv6 routing table, use the **show ipv6 route** command in user EXEC or privileged EXEC mode.

```
show ipv6 route [{ipv6-address | ipv6-prefix/prefix-length [{longer-prefixes}] | [{protocol}] | [repair] | [{updated [{boot-up}] [{day month}] [{time}]}] | interface type number | nd | nsf | table table-id | watch}]
```

Syntax Description

<i>ipv6-address</i>	(Optional) Displays routing information for a specific IPv6 address.
<i>ipv6-prefix</i>	(Optional) Displays routing information for a specific IPv6 network.
<i>/prefix-length</i>	(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.
longer-prefixes	(Optional) Displays output for longer prefix entries.
<i>protocol</i>	(Optional) The name of a routing protocol or the keyword connected , local , mobile , or static . If you specify a routing protocol, use one of the following keywords: bgp , isis , eigrp , ospf , or rip .
repair	(Optional) Displays routes with repair paths.
updated	(Optional) Displays routes with time stamps.
boot-up	(Optional) Displays routing information since bootup.
<i>day month</i>	(Optional) Displays routes since the specified day and month.
<i>time</i>	(Optional) Displays routes since the specified time, in <i>hh:mm</i> format.
interface	(Optional) Displays information about the interface.
<i>type</i>	(Optional) Interface type.

number	(Optional) Interface number.
nd	(Optional) Displays only routes from the IPv6 Routing Information Base (RIB) that are owned by Neighbor Discovery (ND).
nsf	(Optional) Displays routes in the nonstop forwarding (NSF) state.
repair	(Optional)
table table-id	(Optional) Displays IPv6 RIB table information for the specified table ID. The table ID must be in hexadecimal format. The range is from 0 to 0xFFFFFFFF.
watch	(Optional) Displays information about route watchers.

Command Default If none of the optional syntax elements is chosen, all IPv6 routing information for all active routing tables is displayed.

Command Modes User EXEC (>)

Privileged EXEC (#)

Command History	Release	Modification
Cisco IOS XE Everest 16.6.1		This command was introduced.

Usage Guidelines The **show ipv6 route** command provides output similar to the **show ip route** command, except that the information is IPv6-specific.

When the *ipv6-address* or *ipv6-prefix/prefix-length* argument is specified, the longest match lookup is performed from the routing table, and only route information for that address or network is displayed. When a routing protocol is specified, only routes for that protocol are displayed. When the **connected**, **local**, **mobile**, or **static** keyword is specified, only the specified type of route is displayed. When the **interface** keyword and *type* and *number* arguments are specified, only routes for the specified interface are displayed.

Examples

The following is sample output from the **show ipv6 route** command when no keywords or arguments are specified:

```
Device# show ipv6 route

IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
      I1 - ISIS L1, I2 - ISIS L2, IA - IIS interarea
B    2001:DB8:4::2/48 [20/0]
      via FE80::A8BB:CCFF:FE02:8B00, Serial6/0
L    2001:DB8:4::3/48 [0/0]
      via ::, Ethernet1/0
C    2001:DB8:4::4/48 [0/0]
      via ::, Ethernet1/0
LC   2001:DB8:4::5/48 [0/0]
      via ::, Loopback0
L    2001:DB8:4::6/48 [0/0]
      via ::, Serial6/0
C    2001:DB8:4::7/48 [0/0]
```

show ipv6 route

```

      via ::, Serial6/0
S  2001:DB8:4::8/48 [1/0]
      via 2001:DB8:1::1, Null1
L  FE80::/10 [0/0]
      via ::, Null0
L  FF00::/8 [0/0]
      via ::, Null0

```

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

Table 84: show ipv6 route Field Descriptions

Field	Description
Codes:	Indicates the protocol that derived the route. Values are as follows: <ul style="list-style-type: none"> • B—BGP derived • C—Connected • I1—ISIS L1—Integrated IS-IS Level 1 derived • I2—ISIS L2—Integrated IS-IS Level 2 derived • IA—ISIS interarea—Integrated IS-IS interarea derived • L—Local • R—RIP derived • S—Static
2001:DB8:4::2/48	Indicates the IPv6 prefix of the remote network.
[20/0]	The first number in brackets is the administrative distance of the information source; the second number is the metric for the route.
via FE80::A8BB:CCFF:FE02:8B00	Specifies the address of the next device to the remote network.

When the *ipv6-address* or *ipv6-prefix/prefix-length* argument is specified, only route information for that address or network is displayed. The following is sample output from the **show ipv6 route** command when IPv6 prefix 2001:DB8::/35 is specified. The fields in the display are self-explanatory.

```

Device# show ipv6 route 2001:DB8::/35

IPv6 Routing Table - 261 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
      I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
B 2001:DB8::/35 [20/3]
      via FE80::60:5C59:9E00:16, Tunnel1

```

When you specify a protocol, only routes for that particular routing protocol are shown. The following is sample output from the **show ipv6 route bgp** command. The fields in the display are self-explanatory.

```
Device# show ipv6 route bgp
```

```
IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
B    2001:DB8:4::4/64 [20/0]
      via FE80::A8BB:CCFF:FE02:8B00, Serial6/0
```

The following is sample output from the **show ipv6 route local** command. The fields in the display are self-explanatory.

```
Device# show ipv6 route local
```

```
IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
L    2001:DB8:4::2/128 [0/0]
      via ::, Ethernet1/0
LC   2001:DB8:4::1/128 [0/0]
      via ::, Loopback0
L    2001:DB8:4::3/128 [0/0]
      via ::, Serial6/0
L    FE80::/10 [0/0]
      via ::, Null0
L    FF00::/8 [0/0]
      via ::, Null0
```

The following is sample output from the **show ipv6 route** command when the 6PE multipath feature is enabled. The fields in the display are self-explanatory.

```
Device# show ipv6 route
```

```
IPv6 Routing Table - default - 19 entries
Codes:C - Connected, L - Local, S - Static, R - RIP, B - BGP
      U - Per-user Static route
      I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
      O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
.
.
.
B    2001:DB8::/64 [200/0]
      via ::FFFF:172.16.0.1
      via ::FFFF:172.30.30.1
```

Related Commands

Command	Description
ipv6 route	Establishes a static IPv6 route.
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 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

show ipv6 routers [interface-type interface-number][conflicts][vrf vrf-name][detail]

Syntax Description	
<i>interface -type</i>	(Optional) Specifies the Interface type.
<i>interface -number</i>	(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 *on-link* refers to a locally reachable address on the link.)

Command Modes User EXEC (>)

Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	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:

```
Device# show ipv6 routers

Device FE80::83B3:60A4 on Tunnel15, 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.

```
Device# 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 85: 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:

```
Device# show ipv6 routers tunnel 5

Device FE80::83B3:60A4 on Tunnel5, last update 5 min
  Hops 0, Lifetime 6000 sec, AddrFlag=0, OtherFlag=0
  Reachable time 0 msec, Retransmit time 0 msec
  Prefix 3FFE:C00:8007::800:207C:4E37/96 autoconfig
    Valid lifetime -1, preferred lifetime -1
```

show ipv6 rpf

Entering the **conflicts** keyword with the **show ipv6 routers** command displays information for devices that are advertising parameters different from the parameters configured for the interface on which the advertisements are being received, as the following sample output shows:

```
Device# show ipv6 routers conflicts

Device FE80::203: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:

```
Device# show ipv6 routers detail

Device FE80::A8BB:CCFF:FE00:5B00 on Ethernet0/0, last update 0 min
  Rank 0x811 (elegible), Default Router
  Hops 64, Lifetime 1800 sec, AddrFlag=0, OtherFlag=0, MTU=1500
  HomeAgentFlag=0, Preference=Medium, trustlevel = 0
  Reachable time 0 (unspecified), Retransmit time 0 (unspecified)
  Prefix 2001::/64 onlink autoconfig
    Valid lifetime 2592000, preferred lifetime 604800
```

show ipv6 rpf

To check Reverse Path Forwarding (RPF) information for a given unicast host address and prefix, use the **show ipv6 rpf** command in user EXEC or privileged EXEC mode.

```
show ipv6 rpf {source-vrf [access-list] | vrf receiver-vrf{source-vrf [access-list] | select}}
```

Syntax Description	<i>source-vrf</i>	Name or address of the virtual routing and forwarding (VRF) on which lookups are to be performed.
	<i>receiver-vrf</i>	Name or address of the VRF in which the lookups originate.
	<i>access-list</i>	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 Everest 16.6.1	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], multiprotocol Border Gateway Protocol [BGP] routing table, or static mroutes), the **show ipv6 rpf** command to display the source from which the information is retrieved.

Examples

The following example displays RPF information for the unicast host with the IPv6 address of 2001::1:1:2:

```
Device# show ipv6 rpf 2001::1:1:2
RPF information for 2001::1:1:2
  RPF interface:Ethernet3/2
  RPF neighbor:FE80::40:1:3
  RPF route/mask:20::/64
  RPF type:Unicast
  RPF recursion count:0
  Metric preference:110
  Metric:30
```

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

Table 86: 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, multiprotocol BGP, 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

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	<i>source-guard-policy</i>	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 Everest 16.6.1		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

Device# show ipv6 source-guard policy policy1

```
Policy policy1 configuration:
data-glean
prefix-guard
address-guard
```

```
Policy policy1 is applied on the following targets:
Target      Type    Policy          Feature        Target range
Et0/0       PORT   policy1        source-guard   vlan all
vlan 100    VLAN   policy1        source-guard   vlan all
```

Related Commands	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	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.		
Release	Modification						
Cisco IOS XE Everest 16.6.1	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:						
	<pre>Device# show ipv6 spd Current mode: normal Queue max threshold: 74, Headroom: 100, Extended Headroom: 10 IPv6 packet queue: 0</pre>						
	The table below describes the significant fields shown in the display.						
	<p>Table 87: show ipv6 spd Field Description</p> <table border="1"> <thead> <tr> <th>Field</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Current mode: normal</td> <td>The current SPD state or mode.</td> </tr> <tr> <td>Queue max threshold: 74</td> <td>The process input queue maximum.</td> </tr> </tbody> </table>	Field	Description	Current mode: normal	The current SPD state or mode.	Queue max threshold: 74	The process input queue maximum.
Field	Description						
Current mode: normal	The current SPD state or mode.						
Queue max threshold: 74	The process input queue maximum.						
Related Commands	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>ipv6 spd queue max-threshold</td> <td>Configures the maximum number of packets in the SPD process input queue.</td> </tr> </tbody> </table>	Command	Description	ipv6 spd queue max-threshold	Configures the maximum number of packets in the SPD process input queue.		
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	<p><i>ipv6-address</i> (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.</p>
---------------------------	--

show ipv6 static

<i>ipv6-prefix</i>	(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.
<i>/prefix-length</i>	(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.
<i>type</i>	(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.
<i>number</i>	(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: <ul style="list-style-type: none"> • 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 (#)

Release	Modification
Cisco IOS XE Everest 16.6.1	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:

```
Device# show ipv6 static
```

```

IPv6 Static routes
Code: * - installed in RIB
* 3000::/16, interface Ethernet1/0, distance 1
* 4000::/16, via nexthop 2001::1::1, distance 1
  5000::/16, interface Ethernet3/0, distance 1
* 5555::/16, via nexthop 4000::1, distance 1
  5555::/16, via nexthop 9999::1, distance 1
* 5555::/16, interface Ethernet2/0, distance 1
* 6000::/16, via nexthop 2007::1, interface Ethernet1/0, distance 1

```

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

Table 88: show ipv6 static Field Descriptions

Field	Description
via nexthop	Specifies the address of the next Device 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:

```

Device# show ipv6 static 2001:200::/35

IPv6 Static routes
Code: * - installed in RIB
* 2001:200::/35, via nexthop 4000::1, distance 1
  2001:200::/35, via nexthop 9999::1, distance 1
* 2001:200::/35, interface Ethernet2/0, distance 1

```

show ipv6 static interface Command: Example

When an interface is supplied, only those static routes with the specified interface as the outgoing interface are displayed. The **interface** keyword may be used with or without the IPv6 address and prefix specified in the command statement.

```
Device# show ipv6 static interface ethernet 3/0
```

IPv6 Static routes Code: * - installed in RIB 5000::/16, interface Ethernet3/0, distance 1

show ipv6 static recursive Command: Example

When the **recursive** keyword is specified, only recursive static routes are displayed:

```
Device# show ipv6 static recursive
```

show ipv6 traffic

IPv6 Static routes Code: * - installed in RIB * 4000::/16, via nexthop 2001:1::1, distance 1 * 5555::/16, via nexthop 4000::1, distance 1 5555::/16, via nexthop 9999::1, distance 1

show ipv6 static detail Command: Example

When the **detail** keyword is specified, the following additional information is displayed:

- For valid recursive routes, the output path set and maximum resolution depth.
- For invalid recursive routes, the reason why the route is not valid.
- For invalid direct or fully specified routes, the reason why the route is not valid.

```
Device# show ipv6 static detail

IPv6 Static routes
Code: * - installed in RIB
* 3000::/16, interface Ethernet1/0, distance 1
* 4000::/16, via nexthop 2001:1::1, distance 1
    Resolves to 1 paths (max depth 1)
    via Ethernet1/0
5000::/16, interface Ethernet3/0, distance 1
    Interface is down
* 5555::/16, via nexthop 4000::1, distance 1
    Resolves to 1 paths (max depth 2)
    via Ethernet1/0
5555::/16, via nexthop 9999::1, distance 1
    Route does not fully resolve
* 5555::/16, interface Ethernet2/0, distance 1
* 6000::/16, via nexthop 2007::1, interface Ethernet1/0, distance 1
```

Related Commands

Command	Description
ipv6 route	Establishes a static IPv6 route.
show ip route	Displays the current state of the routing table.
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.
------------------	--

<i>interface type number</i>	(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 Everest 16.6.1		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:

```
Device# show ipv6 traffic
IPv6 statistics:
Rcvd: 0 total, 0 local destination
      0 source-routed, 0 truncated
      0 format errors, 0 hop count exceeded
      0 bad header, 0 unknown option, 0 bad source
      0 unknown protocol, 0 not a device
      0 fragments, 0 total reassembled
      0 reassembly timeouts, 0 reassembly failures
      0 unicast RPF drop, 0 suppressed RPF drop
Sent: 0 generated, 0 forwarded
      0 fragmented into 0 fragments, 0 failed
      0 encapsulation failed, 0 no route, 0 too big
Mcast: 0 received, 0 sent
ICMP statistics:
Rcvd: 0 input, 0 checksum errors, 0 too short
      0 unknown info type, 0 unknown error type
unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
parameter: 0 error, 0 header, 0 option
      0 hopcount expired, 0 reassembly timeout, 0 too big
      0 echo request, 0 echo reply
      0 group query, 0 group report, 0 group reduce
      0 device solicit, 0 device advert, 0 redirects
```

The following is sample output for the **show ipv6 interface** command without IPv6 CEF running:

```
Device# show ipv6 interface ethernet 0/1/1
Ethernet0/1/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::203:FDFF:FE49:9
  Description: sat-2900a f0/12
  Global unicast address(es):
    7::7, subnet is 7::/32
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:7
    FF02::1:FF49:9
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
```

show ipv6 traffic

```

Input features: RPF
Unicast RPF access-list MINI
Process Switching:
  0 verification drops
  0 suppressed verification drops
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds

```

The following is sample output for the **show ipv6 interface** command with IPv6 CEF running:

```

Device# show ipv6 interface ethernet 0/1/1
Ethernet0/1/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::203:FDFF:FE49:9
  Description: sat-2900a f0/12
  Global unicast address(es):
    7::7, subnet is 7::/32
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:7
    FF02::1:FF49:9
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  Input features: RPF
  Unicast RPF access-list MINI
  Process Switching:
    0 verification drops
    0 suppressed verification drops
  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 89: show ipv6 traffic Field Descriptions

Field	Description
source-routed	Number of source-routed packets.
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.

Field	Description
no route	Counted when the software discards a datagram it did not know how to route.
unreach	Unreachable messages received are as follows: <ul style="list-style-type: none"> • 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 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 Everest 16.6.1	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.

show ipv6 pim tunnel

The PIM encapsulation tunnel is the register tunnel. An encapsulation tunnel is created for every known rendezvous point (RP) on each router. The PIM decapsulation tunnel is the register decapsulation tunnel. A decapsulation tunnel is created on the RP for the address that is configured to be the RP address.

Examples

The following is sample output from the **show ipv6 pim tunnel** command on the RP:

```
Device# show ipv6 pim tunnel
Tunnel0*
  Type :PIM Encap
  RP   :100::1
  Source:100::1
Tunnel0*
  Type :PIM Decap
  RP   :100::1
  Source: -
```

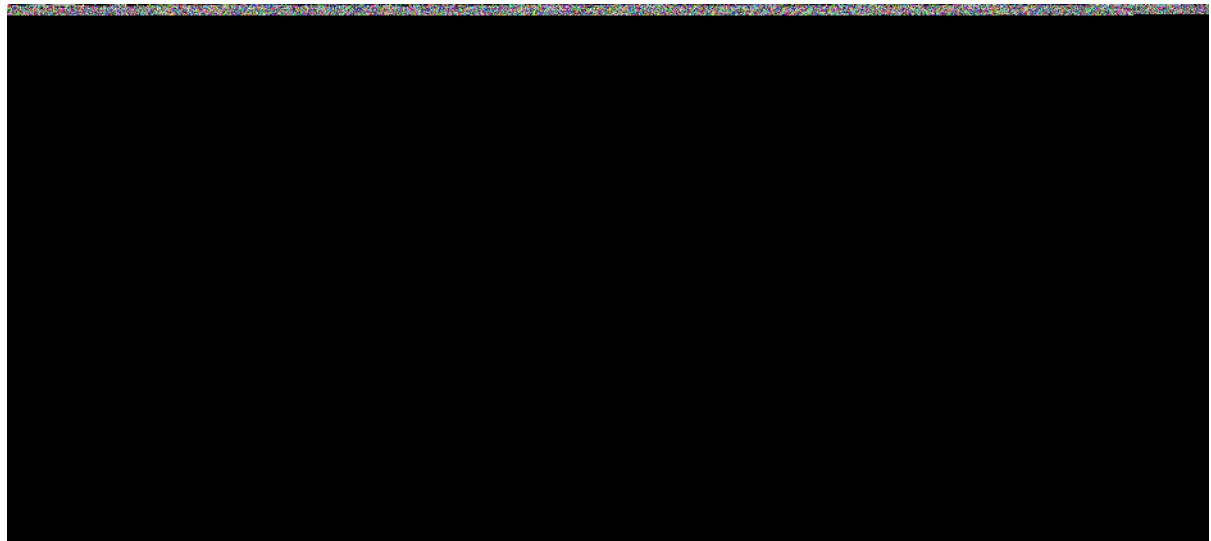
The following is sample output from the **show ipv6 pim tunnel** command on a non-RP:

```
Device# show ipv6 pim tunnel
Tunnel0*
  Type :PIM Encap
  RP   :100::1
  Source:2001::1:1:1
```

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

Table 90: show ipv6 pim tunnel Field Descriptions

Field	Description
Tunnel0*	Name of the tunnel.
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.



PART **VII**

Layer 2/3

- [Layer 2/3 Commands, on page 469](#)

Layer 2/3 Commands

- [channel-group](#), on page 470
- [channel-protocol](#), on page 473
- [clear lacp](#), on page 474
- [clear pagp](#), on page 474
- [clear spanning-tree counters](#), on page 475
- [clear spanning-tree detected-protocols](#), on page 476
- [debug etherchannel](#), on page 476
- [debug lacp](#), on page 477
- [debug pagp](#), on page 478
- [debug platform pm](#), on page 479
- [debug platform udld](#), on page 480
- [debug spanning-tree](#) , on page 480
- [interface port-channel](#), on page 482
- [lacp max-bundle](#), on page 483
- [lacp port-priority](#), on page 484
- [lacp rate](#), on page 485
- [lacp system-priority](#), on page 485
- [pagp learn-method](#), on page 486
- [pagp port-priority](#), on page 487
- [port-channel](#), on page 488
- [port-channel auto](#), on page 489
- [port-channel load-balance](#), on page 489
- [port-channel load-balance extended](#), on page 490
- [port-channel min-links](#), on page 491
- [rep admin vlan](#), on page 492
- [rep block port](#), on page 493
- [rep lsl-age-timer](#), on page 494
- [rep lsl-retries](#), on page 495
- [rep preempt delay](#), on page 495
- [rep preempt segment](#), on page 496
- [rep segment](#), on page 497
- [rep stcn](#), on page 499
- [show etherchannel](#), on page 500

channel-group

- [show interfaces rep detail, on page 502](#)
- [show lacp, on page 503](#)
- [show pagp, on page 507](#)
- [show platform etherchannel, on page 508](#)
- [show platform pm, on page 509](#)
- [show rep topology, on page 509](#)
- [show udld, on page 511](#)
- [switchport, on page 514](#)
- [switchport access vlan, on page 515](#)
- [switchport mode, on page 515](#)
- [switchport nonegotiate, on page 517](#)
- [switchport voice vlan, on page 518](#)
- [udld, on page 521](#)
- [udld port, on page 522](#)
- [udld reset, on page 523](#)

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

<i>channel-group-number</i>	
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 Cisco IOS XE Everest 16.6.1 Modification This command was introduced.
Usage Guidelines	<p>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 <i>channel-group-number</i> can be the same as the <i>port-channel-number</i>, or you can use a new number. If you use a new number, the channel-group command dynamically creates a new port channel.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>If you do not specify non-silent with the auto or desirable mode, silent is assumed. The silent mode is used when the device is connected to a device that is not PAgP-capable and rarely, if ever, sends packets. An example of a silent partner is a file server or a packet analyzer that is not generating traffic. In this case, running PAgP on a physical port prevents that port from ever becoming operational. However, it allows PAgP to operate, to attach the port to a channel group, and to use the port for transmission. Both ends of the link cannot be set to silent.</p> <p>In on mode, a usable EtherChannel exists only when both connected port groups are in the on mode.</p>

channel-group**Caution**

Use care when using the on mode. This is a manual configuration, and ports on both ends of the EtherChannel must have the same configuration. If the group is misconfigured, packet loss or spanning-tree loops can occur.

Passive mode places a port into a negotiating state in which the port responds to received LACP packets but does not initiate LACP packet negotiation. A channel is formed only with another port group in active mode.

Do not configure an EtherChannel in both the PAgP and LACP modes. EtherChannel groups running PAgP and LACP can coexist on the same device or on different devices in the stack (but not in a cross-stack configuration). Individual EtherChannel groups can run either PAgP or LACP, but they cannot interoperate.

If you set the protocol by using the **channel-protocol** interface configuration command, the setting is not overridden by the **channel-group** interface configuration command.

Do not configure a port that is an active or a not-yet-active member of an EtherChannel as an IEEE 802.1x port. If you try to enable IEEE 802.1x authentication on an EtherChannel port, an error message appears, and IEEE 802.1x authentication is not enabled.

Do not configure a secure port as part of an EtherChannel or configure an EtherChannel port as a secure port.

For a complete list of configuration guidelines, see the “Configuring EtherChannels” chapter in the software configuration guide for this release.

Caution

Do not 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 device in the stack. It assigns two static-access ports in VLAN 10 to channel 5 with the PAgP mode desirable:

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

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

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

This example shows how to configure a cross-stack EtherChannel in a device stack. It uses LACP passive mode and assigns two ports on stack member 2 and one port on stack member 3 as static-access ports in VLAN 10 to channel 5:

```
Device# configure terminal
Device(config)# interface range GigabitEthernet 2/0/4 - 5
Device(config-if-range)# switchport mode access
Device(config-if-range)# switchport access vlan 10
```

```

Device(config-if-range)# channel-group 5 mode passive
Device(config-if-range)# exit
Device(config)# interface GigabitEthernet 3/0/3
Device(config-if)# switchport mode access
Device(config-if)# switchport access vlan 10
Device(config-if)# channel-group 5 mode passive
Device(config-if)# exit

```

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

channel-protocol

To restrict the protocol used on a port to manage channeling, use the **channel-protocol** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

```

channel-protocol {lacp | pagp}
no channel-protocol

```

Syntax Description	lacp Configures an EtherChannel with the Link Aggregation Control Protocol (LACP). pagp Configures an EtherChannel with the Port Aggregation Protocol (PAgP).	
Command Default	No protocol is assigned to the EtherChannel.	
Command Modes	Interface configuration	
Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.
Usage Guidelines	<p>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.</p> <p>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.</p> <p>You cannot enable both the PAgP and LACP modes on an EtherChannel group.</p> <p>PAgP and LACP are not compatible; both ends of a channel must use the same protocol.</p> <p>You cannot configure PAgP on cross-stack configurations.</p>	

This example shows how to specify LACP as the protocol that manages the EtherChannel:

```

Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# channel-protocol lacp

```

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

clear lacp

clear lacp

To clear Link Aggregation Control Protocol (LACP) channel-group counters, use the **clear lacp** command in privileged EXEC mode.

clear lacp [channel-group-number] counters

Syntax Description	<i>channel-group-number</i>					
	counters	Clears traffic counters.				
Command Default	None					
Command Modes	Privileged EXEC					
Command History	<table border="1"> <thead> <tr> <th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td><td>This command was introduced.</td></tr> </tbody> </table>		Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification					
Cisco IOS XE Everest 16.6.1	This command was introduced.					

Usage Guidelines You can clear all counters by using the **clear lacp counters** command, or you can clear only the counters for the specified channel group by using the **clear lacp channel-group-number counters** command.

This example shows how to clear all channel-group information:

```
Device# clear lacp counters
```

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

```
Device# clear lacp 4 counters
```

You can verify that the information was deleted by entering the **show lacp counters** or the **show lacp channel-group-number counters** privileged EXEC command.

clear pagp

To clear the Port Aggregation Protocol (PAgP) channel-group information, use the **clear pagp** command in privileged EXEC mode.

clear pagp [channel-group-number] counters

Syntax Description	<i>channel-group-number</i>	
	counters	Clears traffic counters.
Command Default	None	

Command Modes	Privileged EXEC	
Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines You can clear all counters by using the **clear pagp counters** command, or you can clear only the counters for the specified channel group by using the **clear pagp channel-group-number counters** command.

This example shows how to clear all channel-group information:

```
Device# clear pagp counters
```

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

```
Device# clear pagp 10 counters
```

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

clear spanning-tree counters

To clear the spanning-tree counters, use the **clear spanning-tree counters** command in privileged EXEC mode.

clear spanning-tree counters [interface *interface-id*]

Syntax Description	interface <i>interface-id</i>	(Optional) Clears all spanning-tree counters on the specified interface. Valid interfaces include physical ports, VLANs, and port channels. The VLAN range is 1 to 4094.
---------------------------	--------------------------------------	---

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

Command Modes	Privileged EXEC
----------------------	-----------------

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines If the *interface-id* value is not specified, spanning-tree counters are cleared for all interfaces.

This example shows how to clear spanning-tree counters for all interfaces:

```
Device# clear spanning-tree counters
```

clear spanning-tree detected-protocols

clear spanning-tree detected-protocols

To restart the protocol migration process and force renegotiation with neighboring devices on the interface, use the **clear spanning-tree detected-protocols** command in privileged EXEC mode.

clear spanning-tree detected-protocols [interface *interface-id*]

Syntax Description	interface <i>interface-id</i>	(Optional) Restarts the protocol migration process on the specified interface. Valid interfaces include physical ports, VLANs, and port channels. The VLAN range is 1 to 4094.
Command Default	None	
Command Modes	Privileged EXEC	
Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines A device running the rapid per-VLAN spanning-tree plus (rapid-PVST+) protocol or the Multiple Spanning Tree Protocol (MSTP) supports a built-in protocol migration method that enables it to interoperate with legacy IEEE 802.1D devices. If a rapid-PVST+ or an MSTP device receives a legacy IEEE 802.1D configuration bridge protocol data unit (BPDU) with the protocol version set to 0, the device sends only IEEE 802.1D BPDUs on that port. A multiple spanning-tree (MST) device can also detect that a port is at the boundary of a region when it receives a legacy BPDU, an MST BPDU (Version 3) associated with a different region, or a rapid spanning-tree (RST) BPDU (Version 2).

The device does not automatically revert to the rapid-PVST+ or the MSTP mode if it no longer receives IEEE 802.1D BPDUs because it cannot learn whether the legacy switch has been removed from the link unless the legacy switch is the designated switch. Use the **clear spanning-tree detected-protocols** command in this situation.

This example shows how to restart the protocol migration process on a port:

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

debug etherchannel

To enable debugging of EtherChannels, use the **debug etherchannel** command in privileged EXEC mode. To disable debugging, use the **no** form of the command.

```
debug etherchannel [{all | detail | error | event | idb}]
no debug etherchannel [{all | detail | error | event | idb}]
```

Syntax Description	all (Optional) Displays all EtherChannel debug messages. detail (Optional) Displays detailed EtherChannel debug messages. error (Optional) Displays EtherChannel error debug messages. event (Optional) Displays EtherChannel event messages. idb (Optional) Displays PAgP interface descriptor block debug messages.				
Command Default	Debugging is disabled.				
Command Modes	Privileged EXEC				
Command History	<table border="1"> <thead> <tr> <th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td><td>This command was introduced.</td></tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				

Usage Guidelines The **undebbug etherchannel** command is the same as the **no debug etherchannel** command.



Note Although the **linecard** keyword is displayed in the command-line help, it is not supported.

When you enable debugging on a stack, it is enabled only on the active switch. To enable debugging on the standby switch , start a session from the active switch by using the **session switch-number** command in privileged EXEC mode. Enter the **debug** command at the command-line prompt of the standby switch.

To enable debugging on the standby switch without first starting a session on the active switch, use the **remote command** *switch-number LINE* command in privileged EXEC mode.

This example shows how to display all EtherChannel debug messages:

```
Device# debug etherchannel all
```

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

```
Device# debug etherchannel event
```

debug lacp

To enable debugging of Link Aggregation Control Protocol (LACP) activity, use the **debug lacp** command in privileged EXEC mode. To disable LACP debugging, use the **no** form of this command.

```
debug lacp [{all | event | fsm | misc | packet}]
no debug lacp [{all | event | fsm | misc | packet}]
```

Syntax Description	all (Optional) Displays all LACP debug messages. event (Optional) Displays LACP event debug messages.
---------------------------	--

debug pagp

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 Everest 16.6.1	This command was introduced.

Usage Guidelines The **undebug etherchannel** command is the same as the **no debug etherchannel** command.

When you enable debugging on a stack, it is enabled only on the active switch. To enable debugging on the standby switch , start a session from the active switch by using the **session switch-number** command in privileged EXEC mode. Enter the **debug** command at the command-line prompt of the standby switch.

To enable debugging on the standby switch without first starting a session on the active switch, use the **remote command** *switch-number LINE* command in privileged EXEC mode.

This example shows how to display all LACP debug messages:

```
Device# debug LACP all
```

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

```
Device# debug LACP event
```

debug pagp

To enable debugging of Port Aggregation Protocol (PAgP) activity, use the **debug pagp** command in privileged EXEC mode. To disable PAgP debugging, use the **no** form of this command.

```
debug pagp [{all | dual-active | event | fsm | misc | packet}]
no debug pagp [{all | dual-active | event | fsm | misc | packet}]
```

Syntax Description	all	(Optional) Displays all PAgP debug messages.
	dual-active	(Optional) Displays dual-active detection messages.
	event	(Optional) Displays PAgP event debug messages.
	fsm	(Optional) Displays messages about changes within the PAgP finite state machine.
	misc	(Optional) Displays miscellaneous PAgP debug messages.
	packet	(Optional) Displays the receiving and transmitting PAgP control packets.

Command Default	Debugging is disabled.
Command Modes	Privileged EXEC
Command History	Release Cisco IOS XE Everest 16.6.1
	Modification This command was introduced.

Usage Guidelines	The undebbug pagp command is the same as the no debug pagp command. When you enable debugging on a stack, it is enabled only on the active switch. To enable debugging on the standby switch , start a session from the active switch by using the session switch-number command in privileged EXEC mode. Enter the debug command at the command-line prompt of the standby switch. To enable debugging on the standby switch without first starting a session on the active switch, use the remote command switch-number LINE command in privileged EXEC mode.
-------------------------	--

This example shows how to display all PAgP debug messages:

```
Device# debug pagp all
```

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

```
Device# debug pagp event
```

debug platform pm

To enable debugging of the platform-dependent port manager software module, use the **debug platform pm** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

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.
if-numbers	Displays interface-number translation event 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.
vlangs	Displays VLAN creation and deletion event debug messages.

Command Default	Debugging is disabled.
Command Modes	Privileged EXEC

debug platform udld

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines	The undebbug platform pm command is the same as the no debug platform pm command.
	When you enable debugging on a stack, it is enabled only on the active switch. To enable debugging on the standby switch , start a session from the active switch by using the session switch-number command in privileged EXEC mode. Enter the debug command at the command-line prompt of the standby switch.

To enable debugging on the standby switch without first starting a session on the active switch, use the **remote command** *switch-number LINE* command in privileged EXEC mode.

This example shows how to display debug messages related to the creation and deletion of VLANs:

```
Device# debug platform pm vlans
```

debug platform udld

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

Syntax Description	error (Optional) Displays error condition debug messages.	
--------------------	--	--

Command Default	Debugging is disabled.	
-----------------	------------------------	--

Command Modes	Privileged EXEC	
---------------	-----------------	--

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines	The undebbug platform udld command is the same as the no debug platform udld command.	
------------------	---	--

debug spanning-tree

To enable debugging of spanning-tree activities, use the **debug spanning-tree** command in EXEC mode. To disable debugging, use the **no** form of this command.

```
debug spanning-tree {all | backbonefast | bpdu | bpdu-opt | config | etherchannel | events | exceptions | general | ha | mstp | pvst+ | root | snmp | synchronization | switch | uplinkfast}
no debug spanning-tree {all | backbonefast | bpdu | bpdu-opt | config | etherchannel | events | exceptions | general | mstp | pvst+ | root | snmp | synchronization | switch | uplinkfast}
```

Syntax Description	all Displays all spanning-tree debug messages.	
--------------------	---	--

backbonefast	Displays BackboneFast-event debug messages.
bpdu	Displays spanning-tree bridge protocol data unit (BPDU) debug messages.
bpdu-opt	Displays optimized BPDU handling debug messages.
config	Displays spanning-tree configuration change debug messages.
etherchannel	Displays EtherChannel-support debug messages.
events	Displays spanning-tree topology event debug messages.
exceptions	Displays spanning-tree exception debug messages.
general	Displays general spanning-tree activity debug messages.
ha	Displays high-availability spanning-tree debug messages.
mstp	Debugs Multiple Spanning Tree Protocol (MSTP) events.
pvst+	Displays per-VLAN spanning-tree plus (PVST+) event debug messages.
root	Displays spanning-tree root-event debug messages.
snmp	Displays spanning-tree Simple Network Management Protocol (SNMP) handling debug messages.
switch	Displays device shim command debug messages. This shim is the software module that is the interface between the generic Spanning Tree Protocol (STP) code and the platform-specific code of various device platforms.
synchronization	Displays the spanning-tree synchronization event debug messages.
uplinkfast	Displays UplinkFast-event debug messages.

Command Default Debugging is disabled.

Command Modes Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	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.

interface port-channel

To enable debugging on the standby switch without first starting a session on the active switch, use the **remote command** *switch-number LINE* command in privileged EXEC mode.

This example shows how to display all spanning-tree debug messages:

```
Device# debug spanning-tree all
```

interface port-channel

To access or create a port channel, use the **interface port-channel** command in global configuration mode. Use the **no** form of this command to remove the port channel.

```
interface port-channel port-channel-number
no interface port-channel
```

Syntax Description	<i>port-channel-number</i>	
Command Default	No port channel logical interfaces are defined.	
Command Modes	Global configuration	
Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.
Usage Guidelines	<p>For Layer 2 EtherChannels, you do not have to create a port-channel interface before assigning physical ports to a channel group. Instead, you can use the channel-group interface configuration command, which automatically creates the port-channel interface when the channel group obtains its first physical port. If you create the port-channel interface first, the <i>channel-group-number</i> can be the same as the <i>port-channel-number</i>, or you can use a new number. If you use a new number, the channel-group command dynamically creates a new port channel.</p> <p>You create Layer 3 port channels by using the interface port-channel command followed by the no switchport interface configuration command. You should manually configure the port-channel logical interface before putting the interface into the channel group.</p> <p>Only one port channel in a channel group is allowed.</p>	
Caution	 <p>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.</p>	
Caution	 <p>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.</p>	
<p>Follow these guidelines when you use the interface port-channel command:</p>		

- If you want to use the Cisco Discovery Protocol (CDP), you must configure it on the physical port and not on the port channel interface.
- Do not configure a port that is an active member of an EtherChannel as an IEEE 802.1x port. If IEEE 802.1x is enabled on a not-yet active port of an EtherChannel, the port does not join the EtherChannel.

For a complete list of configuration guidelines, see the “Configuring EtherChannels” chapter in the software configuration guide for this release.

This example shows how to create a port channel interface with a port channel number of 5:

```
Device(config)# interface port-channel 5
```

You can verify your setting by entering the **show running-config** privileged EXEC or **show etherchannel *channel-group-number* detail** privileged EXEC command.

lacp max-bundle

To define the maximum number of active LACP ports allowed in a port channel, use the **lacp max-bundle** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

```
lacp max-bundle max_bundle_number  
no lacp max-bundle
```

Syntax Description	<i>max_bundle_number</i> The maximum number of active LACP ports in the port channel. The range is 1 to 8. The default is 8.				
Command Default	None				
Command Modes	Interface configuration				
Command History	<table border="1"> <thead> <tr> <th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td></td><td>This command was introduced.</td></tr> </tbody> </table>	Release	Modification		This command was introduced.
Release	Modification				
	This command was introduced.				

Usage Guidelines	An LACP channel group can have up to 16 Ethernet ports of the same type. Up to eight ports can be active, and up to eight ports can be in hot-standby mode. When there are more than eight ports in an LACP channel group, the device on the controlling end of the link uses port priorities to determine which ports are bundled into the channel and which ports are put in hot-standby mode. Port priorities on the other device (the noncontrolling end of the link) are ignored.
-------------------------	--

The **lacp max-bundle** command must specify a number greater than the number specified by the **port-channel min-links** command.

Use the **show etherchannel summary** privileged EXEC command to see which ports are in the hot-standby mode (denoted with an H port-state flag in the output display).

This example shows how to specify a maximum of five active LACP ports in port channel 2:

lacp port-priority

```
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

Cisco IOS XE Everest 16.6.1

Modification

This command was introduced.

Usage Guidelines

The **lacp port-priority** interface configuration command determines which ports are bundled and which ports are put in hot-standby mode when there are more than eight ports in an LACP channel group.

An LACP channel group can have up to 16 Ethernet ports of the same type. Up to eight ports can be active, and up to eight ports can be in standby mode.

In port-priority comparisons, a numerically lower value has a higher priority: When there are more than eight ports in an LACP channel group, the eight ports with the numerically lowest values (highest priority values) for LACP port priority are bundled into the channel group, and the lower-priority ports are put in hot-standby mode. If two or more ports have the same LACP port priority (for example, they are configured with the default setting of 65535), then an internal value for the port number determines the priority.



Note

The LACP port priorities are only effective if the ports are on the device that controls the LACP link. See the **lacp system-priority** global configuration command for determining which device controls the link.

Use the **show lacp internal** privileged EXEC command to display LACP port priorities and internal port number values.

For information about configuring LACP on physical ports, see the configuration guide for this release.

This example shows how to configure the LACP port priority on a port:

```
Device# interface gigabitethernet2/0/1
Device(config-if)# lacp port-priority 1000
```

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

lacp rate

To set the rate at which Link Aggregation Control Protocol (LACP) control packets are ingressed to an LACP-supported interface, use the **lacp rate** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

lacp rate {normal | fast}
no lacp rate

Syntax Description

normal Specifies that LACP control packets are ingressed at the normal rate, every 30 seconds after the link is bundled.

fast Specifies that LACP control packets are ingressed at the fast rate, once every 1 second.

Command Default

The default ingress rate for control packets is 30 seconds after the link is bundled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
	This command was introduced.

Usage Guidelines

Use this command to modify the duration of LACP timeout. The LACP timeout value on Cisco switch is three times the LACP rate configured on the interface. Using the **lacp rate** command, you can select the LACP timeout value for a switch to be either 90 seconds or 3 seconds.

This command is supported only on LACP-enabled interfaces.

This example shows how to specify the fast (1 second) ingress rate on interface GigabitEthernet 0/0:

```
Device(config)# interface gigabitEthernet 0/0
Device(config-if)# lacp rate fast
```

lacp system-priority

To configure the system priority for the Link Aggregation Control Protocol (LACP), use the **lacp system-priority** command in global configuration mode on the device. To return to the default setting, use the **no** form of this command.

lacp system-priority *priority*
no lacp system-priority

Syntax Description

priority System priority for LACP. The range is 1 to 65535.

pagp learn-method

Command Default	The default is 32768.				
Command Modes	Global configuration				
Command History	<table border="1"> <thead> <tr> <th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td><td>This command was introduced.</td></tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				

Usage Guidelines	<p>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.</p> <p>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.</p> <p>The lacp system-priority command applies to all LACP EtherChannels on the device.</p> <p>Use the show etherchannel summary privileged EXEC command to see which ports are in the hot-standby mode (denoted with an H port-state flag in the output display).</p> <p>This example shows how to set the LACP system priority:</p> <pre>Device(config)# lacp system-priority 20000</pre> <p>You can verify your settings by entering the show lacp sys-id privileged EXEC command.</p>
-------------------------	---

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	<table border="1"> <tr> <td>aggregation-port</td><td>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.</td></tr> <tr> <td>physical-port</td><td>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.</td></tr> </table>	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.
aggregation-port	Specifies address learning on the logical port channel. The device sends packets to the source using any port in the EtherChannel. This setting is the default. With aggregation-port learning, it is not important on which physical port the packet arrives.				
physical-port	Specifies address learning on the physical port within the EtherChannel. The device sends packets to the source using the same port in the EtherChannel from which it learned the source address. The other end of the channel uses the same port in the channel for a particular destination MAC or IP address.				

Command Default	The default is aggregation-port (logical port channel).				
Command Modes	Interface configuration				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				
Usage Guidelines	<p>The learn method must be configured the same at both ends of the link.</p> <p>The device supports address learning only on aggregate ports even though the physical-port keyword is provided in the command-line interface (CLI). The pagp learn-method and the pagp port-priority interface configuration commands have no effect on the device hardware, but they are required for PAgP interoperability with devices that only support address learning by physical ports.</p> <p>When the link partner to the device is a physical learner, we recommend that you configure the device as a physical-port learner by using the pagp learn-method physical-port interface configuration command. We also recommend that you set the load-distribution method based on the source MAC address by using the port-channel load-balance src-mac global configuration command. Use the pagp learn-method interface configuration command only in this situation.</p>				

The learn method must be configured the same at both ends of the link.

The device supports address learning only on aggregate ports even though the **physical-port** keyword is provided in the command-line interface (CLI). The **pagp learn-method** and the **pagp port-priority** interface configuration commands have no effect on the device hardware, but they are required for PAgP interoperability with devices that only support address learning by physical ports.

When the link partner to the device is a physical learner, we recommend that you configure the device as a physical-port learner by using the **pagp learn-method physical-port** interface configuration command. We also recommend that you set the load-distribution method based on the source MAC address by using the **port-channel load-balance src-mac** global configuration command. Use the **pagp learn-method** interface configuration command only in this situation.

This example shows how to set the learning method to learn the address on the physical port within the EtherChannel:

```
Device(config-if)# pagp learn-method physical-port
```

This example shows how to set the learning method to learn the address on the port channel within the EtherChannel:

```
Device(config-if)# pagp learn-method aggregation-port
```

You can verify your settings by entering the **show running-config** privileged EXEC command or the **show pagp channel-group-number internal** privileged EXEC command.

pagp port-priority

To select a port over which all Port Aggregation Protocol (PAgP) traffic through the EtherChannel is sent, use the **pagp port-priority** command in interface configuration mode. If all unused ports in the EtherChannel are in hot-standby mode, they can be placed into operation if the currently selected port and link fails. To return to the default setting, use the **no** form of this command.

```
pagp port-priority priority
no pagp port-priority
```

Syntax Description	<i>priority</i> Priority number. The range is from 0 to 255.
---------------------------	--

Command Default	The default is 128.
------------------------	---------------------

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

port-channel

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.
Usage Guidelines	<p>The physical port with the highest priority that is operational and has membership in the same EtherChannel is the one selected for PAgP transmission.</p> <p>The device supports address learning only on aggregate ports even though the physical-port keyword is provided in the command-line interface (CLI). The pagp learn-method and the pagp port-priority interface configuration commands have no effect on the device hardware, but they are required for PAgP interoperability with devices that only support address learning by physical ports, such as the Catalyst 1900 switch.</p> <p>When the link partner to the device is a physical learner, we recommend that you configure the device as a physical-port learner by using the pagp learn-method physical-port interface configuration command. We also recommend that you set the load-distribution method based on the source MAC address by using the port-channel load-balance src-mac global configuration command. Use the pagp learn-method interface configuration command only in this situation.</p>	
	<p>This example shows how to set the port priority to 200:</p> <pre>Device(config-if)# pagp port-priority 200</pre> <p>You can verify your setting by entering the show running-config privileged EXEC command or the show pagp channel-group-number internal privileged EXEC command.</p>	

port-channel

To convert the auto created EtherChannel into a manual channel and adding configuration on the EtherChannel, use the **port-channel** command in privileged EXEC mode.

port-channel {channel-group-number persistent | persistent}

Syntax Description	<i>channel-group-number</i> Channel group number. The range is 1 to 128.	
	persistent Converts the auto created EtherChannel into a manual channel and allows you to add configuration on the EtherChannel.	
Command Default	None	
Command Modes	Privileged EXEC	
Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.
Usage Guidelines	<p>You can use the show etherchannel summary privileged EXEC command to display the EtherChannel information.</p>	

Examples

This example shows how to convert the auto created EtherChannel into a manual channel:

```
Device# port-channel 1 persistent
```

port-channel auto

To enable the auto-LAG feature on a switch globally, use the **port-channel auto** command in global configuration mode. To disable the auto-LAG feature on the switch globally, use **no** form of this command.

```
port-channel auto
no port-channel auto
```

Syntax Description

This command has no arguments or keywords.

Command Default

By default, the auto-LAG feature is disabled globally and is enabled on all port interfaces.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.7.2E	This command was introduced.

Usage Guidelines

You can use the **show etherchannel auto** privileged EXEC command to verify if the EtherChannel was created automatically.

Examples

This example shows how to enable the auto-LAG feature on the switch:

```
Device(config)# port-channel auto
```

port-channel load-balance

To set the load-distribution method among the ports in the EtherChannel, use the **port-channel load-balance** command in global configuration mode. To reset the load-balancing mechanism to the default setting, use the **no** form of this command.

```
port-channel load-balance {dst-ip | dst-mac | dst-mixed-ip-port | dst-port | extended | src-dst-ip |
src-dst-mac | src-dst-mixed-ip-port | src-dst-port | src-ip | src-mac | src-mixed-ip-port | src-port}
no port-channel load-balance
```

Syntax Description

dst-ip	Specifies load distribution based on the destination host IP address.
dst-mac	Specifies load distribution based on the destination host MAC address. Packets to the same destination are sent on the same port, but packets to different destinations are sent on different ports in the channel.
dst-mixed-ip-port	Specifies load distribution based on the destination IPv4 or IPv6 address and the TCP/UDP (Layer 4) port number.

port-channel load-balance extended

dst-port	Specifies load distribution based on the destination TCP/UDP (Layer 4) port number for both IPv4 and IPv6.
extended	Sets extended load balance methods among the ports in the EtherChannel. See the port-channel load-balance extended command.
src-dst-ip	Specifies load distribution based on the source and destination host IP address.
src-dst-mac	Specifies load distribution based on the source and destination host MAC address.
src-dst-mixed-ip-port	Specifies load distribution based on the source and destination host IP address and TCP/UDP (layer 4) port number.
src-dst-port	Specifies load distribution based on the source and destination TCP/UDP (Layer 4) port number.
src-ip	Specifies load distribution based on the source host IP address.
src-mac	Specifies load distribution based on the source MAC address. Packets from different hosts use different ports in the channel, but packets from the same host use the same port.
src-mixed-ip-port	Specifies load distribution based on the source host IP address and TCP/UDP (Layer 4) port number.
src-port	Specifies load distribution based on the TCP/UDP (Layer 4) port number.

Command Default	The default is src-mac .				
Command Modes	Global configuration				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td> <td>This command was introduced.</td></tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				
Usage Guidelines	You can verify your setting by entering the show running-config privileged EXEC command or the show etherchannel load-balance privileged EXEC command.				
Examples	This example shows how to set the load-distribution method to dst-mac: Device(config)# port-channel load-balance dst-mac				

port-channel load-balance extended

To set combinations of load-distribution methods among the ports in the EtherChannel, use the **port-channel load-balance extended** command in global configuration mode. To reset the extended load-balancing mechanism to the default setting, use the **no** form of this command.

```
port-channel load-balance extended[ {dst-ip | dst-mac | dst-port | ipv6-label | l3-proto | src-ip | src-mac | src-port} ]
```

no port-channel load-balance extended

Syntax Description	dst-ip (Optional) Specifies load distribution based on the destination host IP address. dst-mac (Optional) Specifies load distribution based on the destination host MAC address. Packets to the same destination are sent on the same port, but packets to different destinations are sent on different ports in the channel. dst-port (Optional) Specifies load distribution based on the destination TCP/UDP (Layer 4) port number for both IPv4 and IPv6. ipv6-label (Optional) Specifies load distribution based on the source MAC address and IPv6 flow label. l3-proto (Optional) Specifies load distribution based on the source MAC address and Layer 3 protocols. src-ip (Optional) Specifies load distribution based on the source host IP address. src-mac (Optional) Specifies load distribution based on the source MAC address. Packets from different hosts use different ports in the channel, but packets from the same host use the same port. src-port (Optional) Specifies load distribution based on the TCP/UDP (Layer 4) port number.
---------------------------	--

Command Default The default is **src-mac**.

Command Modes Global configuration

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines For information about when to use these forwarding methods, see the [Forwarding Methods](#) for this release.

You can verify your setting by entering the **show running-config** privileged EXEC command or the **show etherchannel load-balance** privileged EXEC command.

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

```
Device(config)# port-channel load-balance extended dst-ip dst-mac src-ip
```

port-channel min-links

To define the minimum number of LACP ports that must be bundled in the link-up state and bundled in the EtherChannel in order that a port channel becomes active, use the **port-channel min-links** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

```
port-channel min-links min_links_number
no port-channel min-links
```

Syntax Description	<i>min_links_number</i> The minimum number of active LACP ports in the port channel. The range is 2 to 8. The default is 1.
---------------------------	---

rep admin vlan

Command Default	None				
Command Modes	Interface configuration				
Command History	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; padding: 2px;">Release</th> <th style="text-align: right; padding: 2px;">Modification</th> </tr> </thead> <tbody> <tr> <td style="padding: 2px;"></td> <td style="text-align: right; padding: 2px;">This command was introduced.</td> </tr> </tbody> </table>	Release	Modification		This command was introduced.
Release	Modification				
	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 less than the number specified by the **lacp max-bundle** command.

Use the **show etherchannel summary** privileged EXEC command to see which ports are in the hot-standby mode (denoted with an H port-state flag in the output display).

This example shows how to specify a minimum of three active LACP ports before port channel 2 becomes active:

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

rep admin vlan

To configure a Resilient Ethernet Protocol (REP) administrative VLAN for 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 Default None.

Command Modes Global configuration (config)

Command History

Release	Modification
	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(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 <i>port-id</i>	Specifies the VLAN blocking alternate port by entering the unique port ID, which is automatically generated when REP is enabled. The REP port ID is a 16-character hexadecimal value.
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 (config-if)

Command History

Release	Modification
	This command was introduced.

rep Isl-age-timer**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(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 Isl-age-timer

To configure the Resilient Ethernet Protocol (REP) link status layer (LSL) age-out timer value, use the **rep Isl-age-timer** command in interface configuration mode. To restore the default age-out timer value, use the **no** form of this command.

```
rep Isl-age-timer milliseconds
no rep Isl-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 (config-if)

Command History

Release	Modification
---------	--------------

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(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 Isl-retries

To configure the REP link status layer (LSL) number of retries, use the **rep Isl-retries** command in interface configuration mode. To restore the default number of retries, use the **no** form of this command.

```
rep Isl-retries number-of-retries
no rep Isl-retries number-of-retries
```

Syntax Description

number-of-retries Number of LSL retries. The range of retries is from 3 to 10.

Command Default

The default number of LSL retries is 5.

Command Modes

Interface configuration (config-if)

Command History

Release

Modification

This command was introduced

Usage Guidelines

The **rep Isl-retries** command is used to configure the number of retries before the REP link is disabled. While configuring REP configurable timers, we recommend that you configure the REP LSL number of retries first and then configure the REP LSL age-out timer value.

The following example shows how to configure REP LSL retries.

```
Device(config)# interface TenGigabitEthernet 4/1
Device(config-if)# rep segment 2 edge primary
```

rep preempt delay

To configure a waiting period after a segment port failure and recovery before 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 segment

```
rep preempt delay seconds
no rep preempt delay
```

Syntax Description

seconds Number of seconds to delay REP preemption. The range is from 15 to 300 seconds. The default is manual preemption without delay.

Command Default

REP preemption delay is not set. The default is manual preemption without delay.

Command Modes

Interface configuration (config-if)

Command History**Release****Modification**

This command was introduced.

Usage Guidelines

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** interface configuration command) and prepares the segment for the new topology. The configured VLAN list is blocked at the alternate port, and all other VLANs are blocked at the primary edge port.

You can verify your settings by entering the **show interfaces rep** command.

Examples

The following example shows how to configure a REP preemption time delay of 100 seconds on the primary edge port:

```
Device(config)# interface TenGigabitEthernet 4/1
Device(config-if)# rep preempt delay 100
```

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
	This command was introduced.	
Usage Guidelines	<p>Enter this command on the segment, which has the primary edge port on the device.</p> <p>Ensure that all the other segment configurations are completed before setting preemption for VLAN load balancing. When you enter the rep preempt segment <i>segment-id</i> command, a confirmation message appears before the command is executed because preemption for VLAN load balancing can disrupt the network.</p> <p>If you do not enter the rep preempt delay <i>seconds</i> 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.</p> <p>Enter the show rep topology command in privileged EXEC mode to see which port in the segment is the primary edge port.</p> <p>If you do not configure VLAN load balancing, entering the rep preempt segment <i>segment-id</i> command results in the default behavior, that is, the primary edge port blocks all the VLANs.</p> <p>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.</p>	

Examples

The following example shows how to manually trigger REP preemption on segment 100:

```
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	<p>segment-id Segment for which REP is enabled. Assign a segment ID to the interface. The range is from 1 to 1024.</p> <p>edge (Optional) Configures the port as an edge port. Each segment has only two edge ports.</p> <p>no-neighbor (Optional) Specifies the segment edge as one with no external REP neighbor.</p> <p>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.</p> <p>preferred (Optional) Specifies that the port is the preferred alternate port or the preferred port for VLAN load balancing.</p> <p>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.</p>				
Command Default	REP is disabled on the interface.				
Command Modes	Interface configuration (config-if)				
Command History	<table border="1"> <thead> <tr> <th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td></td><td>This command was introduced.</td></tr> </tbody> </table>	Release	Modification		This command was introduced.
Release	Modification				
	This command was introduced.				
Usage Guidelines	<p>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.</p> <p>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:</p> <ul style="list-style-type: none"> • 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:				
	<pre>Device(config)# interface TenGigabitEthernet 4/1 Device(config-if)# rep segment 100</pre>				
	The following example shows how to enable REP on a port and identify the port as the REP primary edge port:				

```
Device(config)# interface TenGigabitEthernet 4/1
Device(config-if)# rep segment 100 edge primary
```

The following example shows how to enable REP on a port and identify the port as the REP secondary edge port:

```
Device(config)# interface TenGigabitEthernet 4/1
Device(config-if)# rep segment 100 edge
```

The following example shows how to enable REP as an edge no-neighbor port:

```
Device(config)# interface TenGigabitEthernet 4/1
Device(config-if)# rep segment 1 edge no-neighbor primary
```

rep stcn

To configure a 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 <i>interface-id</i> Specifies a physical interface or port channel to receive STCNs.				
	segment <i>segment-id-list</i> 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 (config-if)				
Command History	<table border="0"> <tr> <td>Release</td> <td>Modification</td> </tr> <tr> <td></td> <td>This command was introduced.</td> </tr> </table>	Release	Modification		This command was introduced.
Release	Modification				
	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:				
	<pre>Device(config)# interface TenGigabitEthernet 4/1 Device(config-if)# rep stcn segment 25-50</pre>				

show etherchannel

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

<i>channel-group-number</i>	
detail	(Optional) Displays detailed EtherChannel information.
load-balance	(Optional) Displays the load-balance or frame-distribution scheme among ports in the port channel.
port	(Optional) Displays EtherChannel port information.
port-channel	(Optional) Displays port-channel information.
protocol	(Optional) Displays the protocol that is being used in the channel.
summary	(Optional) Displays a one-line summary per channel group.

Command Default

None

Command Modes

User EXEC

Command History

Release	Modification
Cisco IOS XE Everest 16.6.1	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      =       OLoad = 0x00        Protocol = LACP
```

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

Local information:

Port	Flags	State	LACP port Priority	Admin Key	Oper Key	Port Number	Port 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

show interfaces rep detail

```

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	<i>interface-id</i> (Optional) Physical interface used to display the port ID.	
Command Default	None.	
Command Modes	Privileged EXEC (#)	
Command History	Release	Modification
		This command was introduced.
Usage Guidelines	Enter this command on a segment edge port to send STCNs to one or more segments or to an interface. You can verify your settings by entering the show interfaces rep detail command in privileged EXEC mode.	
Examples	The following example shows how to display the REP configuration and status for a specified interface;	
	<pre> Device# show interfaces TenGigabitEthernet4/1 rep detail TenGigabitEthernet4/1 REP enabled Segment-id: 3 (Primary Edge) PortID: 03010015FA66FF80 </pre>	

```

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 lacp

To display Link Aggregation Control Protocol (LACP) channel-group information, use the **show lacp** command in user EXEC mode.

show lacp [channel-group-number] {counters | internal | neighbor | sys-id}

Syntax Description	<i>channel-group-number</i> counters Displays traffic information. internal Displays internal information. neighbor Displays neighbor information. sys-id Displays the system identifier that is being used by LACP. The system identifier consists of the LACP system priority and the device MAC address.
---------------------------	---

Command Default	None				
Command Modes	User EXEC				
Command History	<table border="0"> <tr> <td>Release</td> <td>Modification</td> </tr> <tr> <td>Cisco IOS XE Everest 16.6.1</td> <td>This command was introduced.</td> </tr> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	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.
-------------------------	--

show lacp

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.

Port	LACPDU Sent		Marker Sent		Marker Response Sent		LACPDU Recv	
	Sent	Recv	Sent	Recv	Sent	Recv	Pkts	Err
Channel group:1								
Gi2/0/1	19	10	0	0	0	0	0	0
Gi2/0/2	14	6	0	0	0	0	0	0

Table 91: show lacp counters Field Descriptions

Field	Description
LACPDU Sent and Recv	The number of LACP packets sent and received by a port.
Marker Sent and Recv	The number of LACP marker packets sent and received by a port.
Marker Response Sent and Recv	The number of LACP marker response packets sent and received by a port.
LACPDU 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:

Flags: S - Device is requesting Slow LACPDU F - Device is requesting Fast LACPDU A - Device is in Active mode P - Device is in Passive mode								
Channel group 1								
Port	Flags	State	LACP port Priority	Admin Key	Oper Key	Port Number	Port 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 92: show lacp internal Field Descriptions

Field	Description
State	<p>State of the specific port. These are the allowed values:</p> <ul style="list-style-type: none"> • --—Port is in an unknown state. • bndl—Port is attached to an aggregator and bundled with other ports. • susp—Port is in a suspended state; it is not attached to any aggregator. • hot-sby—Port is in a hot-standby state. • indiv—Port is incapable of bundling with any other port. • indep—Port is in an independent state (not bundled but able to handle data traffic. In this case, LACP is not running on the partner port). • down—Port is down.
LACP Port Priority	Port priority setting. LACP uses the port priority to put ports in standby mode when there is a hardware limitation that prevents all compatible ports from aggregating.
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.

show lacp

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

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

```
Device> show lacp neighbor
Flags: S - Device is sending Slow LACPDU F - Device is sending Fast LACPDU
       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

<i>channel-group-number</i>	
counters	Displays traffic information.
dual-active	Displays the dual-active status.
internal	Displays internal information.
neighbor	Displays neighbor information.

Command Default

None

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines

You can enter any **show pagp** command to display the active channel-group information. To display the nonactive information, enter the **show pagp** command with a channel-group number.

Examples

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

```
Device> show pagp 1 counters
          Information      Flush
Port      Sent    Recv      Sent    Recv
-----
Channel group: 1
  Gi1/0/1    45      42      0      0
  Gi1/0/2    45      41      0      0
```

This is an example of output from the **show pagp dual-active** command:

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

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

show platform etherchannel

<output truncated>

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

```
Device> show pagp 1 internal
Flags: S - Device is sending Slow hello. C - Device is in Consistent state.
       A - Device is in Auto mode.
Timers: H - Hello timer is running.          Q - Quit timer is running.
       S - Switching timer is running.        I - Interface timer is running.

Channel group 1
Port      Flags State   Timers  Hello Interval Partner Count PAgP Priority Learning Method Ifindex
Gi1/0/1   SC    U6/S7   H       30s     1        128      Any      16
Gi1/0/2   SC    U6/S7   H       30s     1        128      Any      16
```

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

```
Device> show pagp 1 neighbor
Flags: S - Device is sending Slow hello. C - Device is in Consistent state.
       A - Device is in Auto mode.          P - Device learns on physical port.

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

show platform etherchannel

To display platform-dependent EtherChannel information, use the **show platform etherchannel** command in privileged EXEC mode.

```
show platform etherchannel channel-group-number {group-mask | load-balance mac src-mac dst-mac [ip src-ip dst-ip [port src-port dst-port]]} [switch switch-number]
```

Syntax Description

channel-group-number Channel group number. The range is 1 to 128.

group-mask Displays EtherChannel group mask.

load-balance Tests EtherChannel load-balance hash algorithm.

mac *src-mac dst-mac* Specifies the source and destination MAC addresses.

ip *src-ip dst-ip* (Optional) Specifies the source and destination IP addresses.

port *src-port dst-port* (Optional) Specifies the source and destination layer port numbers.

switch *switch-number* (Optional) Specifies the stack member.

Command Default	None				
Command Modes	Privileged EXEC				
Command History	<table border="1"> <thead> <tr> <th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td><td>This command was introduced.</td></tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				

Usage Guidelines Use this command only when you are working directly with a technical support representative while troubleshooting a problem.

Do not use this command unless a technical support representative asks you to do so.

show platform pm

To display platform-dependent port manager information, use the **show platform pm** command in privileged EXEC mode.

Command Default	None				
Command Modes	Privileged EXEC				
Command History	<table border="1"> <thead> <tr> <th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td><td>This command was introduced.</td></tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	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 <i>segment-id</i>	(Optional) Specifies the segment for which to display the REP topology information. The <i>segment-id</i> 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 (#)	

show rep topology

Command History	Release	Modification
		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 udld

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

```
show udld [Auto-Template | Capwap | GigabitEthernet | GroupVI | InternalInterface | Loopback | Null | Port-channel | TenGigabitEthernet | Tunnel | Vlan] interface_number
show udld neighbors
```

Syntax Description		
	Auto-Template	(Optional) Displays UDLD operational status of the auto-template interface. The range is from 1 to 999.
	Capwap	(Optional) Displays UDLD operational status of the CAPWAP interface. The range is from 0 to 2147483647.
	GigabitEthernet	(Optional) Displays UDLD operational status of the GigabitEthernet interface. The range is from 0 to 9.
	GroupVI	(Optional) Displays UDLD operational status of the group virtual interface. The range is from 1 to 255.
	InternalInterface	(Optional) Displays UDLD operational status of the internal interface. The range is from 0 to 9.
	Loopback	(Optional) Displays UDLD operational status of the loopback interface. The range is from 0 to 2147483647.
	Null	(Optional) Displays UDLD operational status of the null interface.
	Port-channel	(Optional) Displays UDLD operational status of the Ethernet channel interfaces. The range is from 1 to 128.
	TenGigabitEthernet	(Optional) Displays UDLD operational status of the Ten Gigabit Ethernet interface. The range is from 0 to 9.
	Tunnel	(Optional) Displays UDLD operational status of the tunnel interface. The range is from 0 to 2147483647.
	Vlan	(Optional) Displays UDLD operational status of the VLAN interface. The range is from 1 to 4095.
	<i>interface-id</i>	(Optional) ID of the interface and port number. Valid interfaces include physical ports, VLANs, and port channels.

show udld

neighbors	(Optional) Displays neighbor information only.				
Command Default	None				
Command Modes	User EXEC				
Command History	<table border="1"> <thead> <tr> <th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td><td>This command was introduced.</td></tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	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.				
	<pre>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</pre>				

Table 93: 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.

Field	Description
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.
Current operational state	The current phase of the UDLD state machine. For a normal bidirectional link, the state machine is most often in the Advertisement phase.
Message interval	How often advertisement messages are sent from the local device. Measured in seconds.
Time out interval	The time period, in seconds, that UDLD waits for echoes from a neighbor device during the detection window.
Entry 1	Information from the first cache entry, which contains a copy of echo information received from the neighbor.
Expiration time	The amount of time in seconds remaining before this cache entry is aged out.
Device ID	The neighbor device identification.
Current neighbor state	The neighbor's current state. If both the local and neighbor devices are running UDLD normally, the neighbor state and local state should be bidirectional. If the link is down or the neighbor is not UDLD-capable, no cache entries appear.
Device name	The device name or the system serial number of the neighbor. The system serial number appears if the device name is not set or is set to the default (Switch).
Port ID	The neighbor port ID enabled for UDLD.
Neighbor echo 1 device	The device name of the neighbors' neighbor from which the echo originated.
Neighbor echo 1 port	The port number ID of the neighbor from which the echo originated.
Message interval	The rate, in seconds, at which the neighbor is sending advertisement messages.
CDP device name	The CDP device name or the system serial number. The system serial number appears if the device name is not set or is set to the default (Switch).

This is an example of output from the **show udld neighbors** command:

```
Device# show udld neighbors
Port      Device Name        Device ID  Port-ID  OperState
-----  -----
Gi2/0/1   Switch-A          1          Gi2/0/1  Bidirectional
Gi3/0/1   Switch-A          2          Gi3/0/1  Bidirectional
```

switchport

To put an interface that is in Layer 3 mode into Layer 2 mode for Layer 2 configuration, use the **switchport** command in interface configuration mode. To put an interface in Layer 3 mode, use the **no** form of this command.

switchport
no switchport

Syntax Description This command has no arguments or keywords.

Command Default By default, all interfaces are in Layer 2 mode.

Command Modes Interface configuration

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines Use the **no switchport** command (without parameters) to set the interface to the routed-interface status and to erase all Layer 2 configurations. You must use this command before assigning an IP address to a routed port.



Note This command is not supported on devices running the LAN Base feature set.

Entering the **no switchport** command shuts the port down and then reenables it, which might generate messages on the device to which the port is connected.

When you put an interface that is in Layer 2 mode into Layer 3 mode (or the reverse), the previous configuration information related to the affected interface might be lost, and the interface is returned to its default configuration.



Note If an interface is configured as a Layer 3 interface, you must first enter the **switchport** command to configure the interface as a Layer 2 port. Then you can enter the **switchport access vlan** and **switchport mode** commands.

The **switchport** command is not used on platforms that do not support Cisco-routed ports. All physical ports on such platforms are assumed to be Layer 2-switched interfaces.

You can verify the port status of an interface by entering the **show running-config** privileged EXEC command.

Examples

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

```
Device(config-if)# no switchport
```

This example shows how to cause the port interface to cease operating as a Cisco-routed port and convert to a Layer 2 switched interface:

```
Device(config-if)# switchport
```

switchport access vlan

To configure a port as a static-access port, use the **switchport access vlan** command in interface configuration mode. To reset the access mode to the default VLAN mode for the device, use the **no** form of this command.

```
switchport access vlan {vlan-id}
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 Everest 16.6.1	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(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

```
switchport mode {access | dynamic | {auto | desirable} | trunk}
noswitchport mode {access | dynamic | {auto | desirable} | trunk}
```

Syntax Description	access Sets the port to access mode (either static-access or dynamic-access depending on the setting of the switchport access vlan interface configuration command). The port is set to access unconditionally and operates as a nontrunking, single VLAN interface that sends and receives nonencapsulated (non-tagged) frames. An access port can be assigned to only one VLAN. dynamic auto Sets the port trunking mode dynamic parameter to auto to specify that the interface convert the link to a trunk link. This is the default switchport mode. dynamic desirable Sets the port trunking mode dynamic parameter to desirable to specify that the interface actively attempt to convert the link to a trunk link. trunk Sets the port to trunk unconditionally. The port is a trunking VLAN Layer 2 interface. The port sends and receives encapsulated (tagged) frames that identify the VLAN of origination. A trunk is a point-to-point link between two devices or between a device and a router.				
Command Default	The default mode is dynamic auto .				
Command Modes	Interface configuration				
Command History	<table border="1"> <thead> <tr> <th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td><td>This command was introduced.</td></tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				
Usage Guidelines	<p>A configuration that uses the access, or trunk keywords takes effect only when you configure the port in the appropriate mode by using the switchport mode command. The static-access and trunk configuration are saved, but only one configuration is active at a time.</p> <p>When you enter access mode, the interface changes to permanent nontrunking mode and negotiates to convert the link into a nontrunk link even if the neighboring interface does not agree to the change.</p> <p>When you enter trunk mode, the interface changes to permanent trunking mode and negotiates to convert the link into a trunk link even if the interface connecting to it does not agree to the change.</p> <p>When you enter dynamic auto mode, the interface converts the link to a trunk link if the neighboring interface is set to trunk or desirable mode.</p> <p>When you enter dynamic desirable mode, the interface becomes a trunk interface if the neighboring interface is set to trunk, desirable, or auto mode.</p> <p>To autonegotiate trunking, the interfaces must be in the same VLAN Trunking Protocol (VTP) domain. Trunk negotiation is managed by the Dynamic Trunking Protocol (DTP), which is a point-to-point protocol. However, some internetworking devices might forward DTP frames improperly, which could cause misconfigurations. To avoid this problem, configure interfaces connected to devices that do not support DTP to not forward DTP frames, which turns off DTP.</p> <ul style="list-style-type: none"> If you do not intend to trunk across those links, use the switchport mode access interface configuration command to disable trunking. 				

- To enable trunking to a device that does not support DTP, use the **switchport mode trunk** and **switchport nonegotiate** interface configuration commands to cause the interface to become a trunk but to not generate DTP frames.

Access ports and trunk ports are mutually exclusive.

The IEEE 802.1x feature interacts with switchport modes in these ways:

- If you try to enable IEEE 802.1x on a trunk port, an error message appears, and IEEE 802.1x is not enabled. If you try to change the mode of an IEEE 802.1x-enabled port to trunk, the port mode is not changed.
- If you try to enable IEEE 802.1x on a port set to **dynamic auto** or **dynamic desirable**, an error message appears, and IEEE 802.1x is not enabled. If you try to change the mode of an IEEE 802.1x-enabled port to **dynamic auto** or **dynamic desirable**, the port mode is not changed.
- If you try to enable IEEE 802.1x on a dynamic-access (VLAN Query Protocol [VQP]) port, an error message appears, and IEEE 802.1x is not enabled. If you try to change an IEEE 802.1x-enabled port to dynamic VLAN assignment, an error message appears, and the VLAN configuration is not changed.

You can verify your settings by entering the **show interfaces interface-id switchport** privileged EXEC command and examining information in the *Administrative Mode* and *Operational Mode* rows.

Examples

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

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

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

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

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

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

switchport nonegotiate

To specify that Dynamic Trunking Protocol (DTP) negotiation packets are not sent on the Layer 2 interface, use the **switchport nonegotiate** command in interface configuration mode. Use the **no** form of this command to return to the default setting.

switchport nonegotiate
no switchport nonegotiate

Syntax Description

This command has no arguments or keywords.

Command Default

The default is to use DTP negotiation to learn the trunking status.

Command Modes

Interface configuration

switchport voice vlan

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines	The no switchport nonegotiate command removes nonegotiate status.
	This command is valid only when the interface switchport mode is access or trunk (configured by using the switchport mode access or the switchport mode trunk interface configuration command). This command returns an error if you attempt to execute it in dynamic (auto or desirable) mode.

Internetworking devices that do not support DTP might forward DTP frames improperly and cause misconfigurations. To avoid this problem, turn off DTP by using the **switchport nonegotiate** command to configure the interfaces connected to devices that do not support DTP to not forward DTP frames.

When you enter the **switchport nonegotiate** command, DTP negotiation packets are not sent on the interface. The device does or does not trunk according to the **mode** parameter: **access** or **trunk**.

- If you do not intend to trunk across those links, use the **switchport mode access** interface configuration command to disable trunking.
- To enable trunking on a device that does not support DTP, use the **switchport mode trunk** and **switchport nonegotiate** interface configuration commands to cause the interface to become a trunk but to not generate DTP frames.

This example shows how to cause a port to refrain from negotiating trunking mode and to act as a trunk or access port (depending on the mode set):

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

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

switchport voice vlan

To configure voice VLAN on the port, use the **switchport voice vlan** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

```
switchport voice vlan {vlan-id | dot1p | none | untagged | name vlan_name}
no switchport voice vlan
```

Syntax Description	vlan-id The VLAN to be used for voice traffic. The range is 1 to 4094. By default, the IP phone forwards the voice traffic with an IEEE 802.1Q priority of 5.
	dot1p Configures the telephone to use IEEE 802.1p priority tagging and uses VLAN 0 (the native VLAN). By default, the Cisco IP phone forwards the voice traffic with an IEEE 802.1p priority of 5.
	none Does not instruct the IP telephone about the voice VLAN. The telephone uses the configuration from the telephone key pad.

untagged	Configures the telephone to send untagged voice traffic. This is the default for the telephone.
name <i>vlan_name</i>	(Optional) Specifies the VLAN name to be used for voice traffic. You can enter up to 128 characters.

Command Default The default is not to automatically configure the telephone (**none**).

The telephone default is not to tag frames.

Command Modes Interface configuration

Command History	Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced.	Option to specify a VLAN name for voice VLAN. The ' name ' keyword was added.

Usage Guidelines You should configure voice VLAN on Layer 2 access ports.

You must enable Cisco Discovery Protocol (CDP) on the switch port connected to the Cisco IP phone for the device to send configuration information to the phone. CDP is enabled by default globally and on the interface.

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 shows how to first populate the VLAN database by associating a VLAN ID with a VLAN name, and then configure the VLAN (using the name) on an interface, in the access mode: You can also verify your configuration by entering the **show interfaces *interface-id* switchport** in privileged EXEC command and examining information in the Voice VLAN: row.

Part 1 - Making the entry in the VLAN database:

```
Device# configure terminal
Device(config)# vlan 55
Device(config-vlan)# name test
```

switchport voice vlan

```
Device(config-vlan)# end
Device#
```

Part 2 - Checking the VLAN database:

```
Device# show vlan id 55
VLAN Name Status Ports
-----
55 test active
VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
-----
55 enet 100055 1500 - - - - 0 0
Remote SPAN VLAN
-----
Disabled
Primary Secondary Type Ports
-----
```

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

```
Device# configure terminal
Device(config)# interface gigabitethernet3/1/1
Device(config-if)# switchport mode access
Device(config-if)# switchport voice vlan name test
Device(config-if)# end
Device#
```

Part 4 - Verifying configuration:

```
Device# show running-config
interface gigabitethernet3/1/1
Building configuration...
Current configuration : 113 bytes
!
interface GigabitEthernet3/1/1
switchport voice vlan 55
switchport mode access
Switch#
```

Part 5 - Also can be verified in interface switchport:

```
Device# show interface GigabitEthernet3/1/1 switchport
Name: Gi3/1/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: 55 (test)
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
```

```
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
Device#
```

udld

To enable aggressive or normal mode in the UniDirectional Link Detection (UDLD) and to set the configurable message timer time, use the **udld** command in global configuration mode. To disable aggressive or normal mode UDLD on all fiber-optic ports, use the **no** form of the command.

```
udld {aggressive | enable | message time message-timer-interval}
no udld {aggressive | enable | message}
```

Syntax Description	aggressive Enables UDLD in aggressive mode on all fiber-optic interfaces. enable Enables UDLD in normal mode on all fiber-optic interfaces. message time <i>message-timer-interval</i> Configures the period of time between UDLD probe messages on ports that are in the advertisement phase and are determined to be bidirectional. The range is 1 to 90 seconds. The default is 15 seconds.
---------------------------	--

Command Default UDLD is disabled on all interfaces.

The message timer is set at 15 seconds.

Command Modes Global configuration

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines UDLD supports two modes of operation: normal (the default) and aggressive. In normal mode, UDLD detects unidirectional links due to misconnected interfaces on fiber-optic connections. In aggressive mode, UDLD also detects unidirectional links due to one-way traffic on fiber-optic and twisted-pair links and due to misconnected interfaces on fiber-optic links. For information about normal and aggressive modes, see the *Catalyst 2960-X Switch Layer 2 Configuration Guide* and *Catalyst 2960-XR Switch Layer 2 Configuration Guide*.

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.

udld port

- The **no udld enable** global configuration command followed by the **udld {aggressive | enable}** global configuration command to reenable UDLD globally.
- The **no udld port** interface configuration command followed by the **udld port** or **udld port aggressive** interface configuration command to reenable UDLD on the specified interface.
- The **errdisable recovery cause udld** and **errdisable recovery interval interval** global configuration commands to automatically recover from the UDLD error-disabled state.

This example shows how to enable UDLD on all fiber-optic interfaces:

```
Device(config)# udld enable
```

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

udld port

To enable UniDirectional Link Detection (UDLD) on an individual interface or to prevent a fiber-optic interface from being enabled by the **udld** global configuration command, use the **udld port** command in interface configuration mode. To return to the **udld** global configuration command setting or to disable UDLD if entered for a nonfiber-optic port, use the **no** form of this command.

udld port [aggressive]
no udld port [aggressive]

Syntax Description

aggressive (Optional) Enables UDLD in aggressive mode on the specified interface.

Command Default

On fiber-optic interfaces, UDLD is disabled and fiber-optic interfaces enable UDLD according to the state of the **udld enable** or **udld aggressive** global configuration command.

On nonfiber-optic interfaces, UDLD is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines

A UDLD-capable port cannot detect a unidirectional link if it is connected to a UDLD-incapable port of another device.

UDLD supports two modes of operation: normal (the default) and aggressive. In normal mode, UDLD detects unidirectional links due to misconnected interfaces on fiber-optic connections. In aggressive mode, UDLD also detects unidirectional links due to one-way traffic on fiber-optic and twisted-pair links and due to misconnected interfaces on fiber-optic links.

To enable UDLD in normal mode, use the **udld port** interface configuration command. To enable UDLD in aggressive mode, use the **udld port aggressive** interface configuration command.

Use the **no udld port** command on fiber-optic ports to return control of UDLD to the **udld enable** global configuration command or to disable UDLD on nonfiber-optic ports.

Use the **udld port aggressive** command on fiber-optic ports to override the setting of the **udld enable** or **udld aggressive** global configuration command. Use the **no** form on fiber-optic ports to remove this setting and to return control of UDLD enabling to the **udld** global configuration command or to disable UDLD on nonfiber-optic ports.

You can use these commands to reset an interface shut down by UDLD:

- The **udld reset** privileged EXEC command resets all interfaces shut down by UDLD.
- The **shutdown** and **no shutdown** interface configuration commands.
- The **no udld enable** global configuration command, followed by the **udld {aggressive | enable}** global configuration command reenables UDLD globally.
- The **no udld port** interface configuration command, followed by the **udld port** or **udld port aggressive** interface configuration command reenables UDLD on the specified interface.
- The **errdisable recovery cause udld** and **errdisable recovery interval** *interval* global configuration commands automatically recover from the UDLD error-disabled state.

This example shows how to enable UDLD on an port:

```
Device(config)# interface gigabitethernet6/0/1
Device(config-if)# udld port
```

This example shows how to disable UDLD on a fiber-optic interface despite the setting of the **udld** global configuration command:

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

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

udld reset

To reset all interfaces disabled by UniDirectional Link Detection (UDLD) and permit traffic to begin passing through them again (though other features, such as spanning tree, Port Aggregation Protocol (PAgP), and Dynamic Trunking Protocol (DTP) still have their normal effects, if enabled), use the **udld reset** command in privileged EXEC mode.

udld reset

Syntax Description	This command has no arguments or keywords.
Command Default	None
Command Modes	Privileged EXEC

udld reset

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines	If the interface configuration is still enabled for UDLD, these ports begin to run UDLD again and are disabled for the same reason if the problem has not been corrected.
-------------------------	---

This example shows how to reset all interfaces disabled by UDLD:

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



PART VIII

Multiprotocol Label Switching

- [MPLS Commands, on page 527](#)
- [Multicast VPN Commands, on page 547](#)

CHAPTER ■ ■ ■

MPLS Commands

- [mpls ip default-route](#), on page 527
- [mpls ip \(global configuration\)](#), on page 528
- [mpls ip \(interface configuration\)](#), on page 529
- [mpls label protocol \(global configuration\)](#), on page 530
- [mpls label protocol \(interface configuration\)](#), on page 530
- [mpls label range](#), on page 531
- [mpls static binding ipv4](#), on page 533
- [show mpls forwarding-table](#), on page 535
- [show mpls label range](#), on page 542
- [show mpls static binding](#), on page 542
- [show mpls static crossconnect](#), on page 544

mpls ip default-route

To enable the distribution of labels associated with the IP default route, use the **mpls ip default-route** command in global configuration mode.

mpls ip default-route

Syntax Description This command has no arguments or keywords.

Command Default No distribution of labels for the IP default route.

Command Modes Global configuration

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

Usage Guidelines Dynamic label switching (that is, distribution of labels based on routing protocols) must be enabled before you can use the **mpls ip default-route** command.

mpls ip (global configuration)**Examples**

The following example shows how to enable the distribution of labels associated with the IP default route:

```
Switch# configure terminal
Switch(config)# mpls ip
Switch(config)# mpls ip default-route
```

Related Commands

Command	Description
mpls ip (global configuration)	Enables MPLS forwarding of IPv4 packets along normally routed paths for the platform.
mpls ip (interface configuration)	Enables MPLS forwarding of IPv4 packets along normally routed paths for a particular interface.

mpls ip (global configuration)

To enable Multiprotocol Label Switching (MPLS) forwarding of IPv4 and IPv6 packets along normally routed paths for the platform, use the **mpls ip** command in global configuration mode. To disable this feature, use the **no** form of this command.

```
mpls ip
no mpls ip
```

Syntax Description

This command has no arguments or keywords.

Command Default

Label switching of IPv4 and IPv6 packets along normally routed paths is enabled for the platform.

Command Modes

Global configuration

Command History

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

Usage Guidelines

MPLS forwarding of IPv4 and IPv6 packets along normally routed paths (sometimes called dynamic label switching) is enabled by this command. For a given interface to perform dynamic label switching, this switching function must be enabled for the interface and for the platform.

The **no** form of this command stops dynamic label switching for all platform interfaces regardless of the interface configuration; it also stops distribution of labels for dynamic label switching. However, the no form of this command does not affect the sending of labeled packets through label switch path (LSP) tunnels.

Examples

The following example shows that dynamic label switching is disabled for the platform, and all label distribution is terminated for the platform:

```
Switch(config)# no mpls ip
```

Related Commands	Command	Description
	mpls ip (interface configuration)	Enables MPLS forwarding of IPv4 and IPv6 packets along normally routed paths for the associated interface.

mpls ip (interface configuration)

To enable Multiprotocol Label Switching (MPLS) forwarding of IPv4 and IPv6 packets along normally routed paths for a particular interface, use the **mpls ip** command in interface configuration mode. To disable this configuration, use the **no** form of this command.

mpls ip
no mpls ip

Syntax Description This command has no arguments or keywords.

Command Default MPLS forwarding of IPv4 and IPv6 packets along normally routed paths for the interface is disabled.

Command Modes Interface configuration (config-if)

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

Usage Guidelines MPLS forwarding of IPv4 and IPv6 packets along normally routed paths is sometimes called dynamic label switching. If dynamic label switching has been enabled for the platform when this command is issued on an interface, label distribution for the interface begins with the periodic transmission of neighbor discovery Hello messages on the interface. When the outgoing label for a destination routed through the interface is known, packets for the destination are labeled with that outgoing label and forwarded through the interface.

The **no** form of this command causes packets routed out through the interface to be sent unlabeled; this form of the command also terminates label distribution for the interface. However, the no form of the command does not affect the sending of labeled packets through any link-state packet (LSP) tunnels that might use the interface.

Examples The following example shows how to enable label switching on the specified Ethernet interface:

```
Switch(config)# configure terminal
Switch(config-if)# interface TenGigabitEthernet1/0/3
Switch(config-if)# mpls ip
```

The following example shows that label switching is enabled on the specified vlan interface (SVI) on a Cisco Catalyst switch:

```
Switch(config)# configure terminal
Switch(config-if)# interface vlan 1
Switch(config-if)# mpls ip
```

mpls label protocol (global configuration)

To specify the Label Distribution Protocol (LDP) for a platform, use the **mpls label protocol** command in global configuration mode. To restore the default LDP, use the **no** form of this command.

```
mpls label protocol ldp
no mpls label protocol ldp
```

Syntax Description	ldp Specifies that LDP is the default label distribution protocol.				
Command Default	LDP is the default label distribution protocol.				
Command Modes	Global configuration				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Denali 16.3.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Denali 16.3.1	This command was introduced.
Release	Modification				
Cisco IOS XE Denali 16.3.1	This command was introduced.				

Usage Guidelines If neither the global **mpls label protocol ldp** command nor the interface **mpls label protocol ldp** command is used, all label distribution sessions use LDP.

Examples The following command establishes LDP as the label distribution protocol for the platform:

```
Switch(config)# mpls label protocol ldp
```

mpls label protocol (interface configuration)

To specify the label distribution protocol for an interface, use the **mpls label protocol** command in interface configuration mode. To remove the label distribution protocol from the interface, use the **no** form of this command.

```
mpls label protocol ldp
no mpls label protocol ldp
```

Syntax Description	ldp Specifies that the label distribution protocol (LDP) is to be used on the interface.
Command Default	If no protocol is explicitly configured for an interface, the label distribution protocol that was configured for the platform is used. To set the platform label distribution protocol, use the global mpls label protocol command.
Command Modes	Interface configuration (config-if)

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

Usage Guidelines To successfully establish a session for label distribution for a link connecting two label switch routers (LSRs), the link interfaces on the LSRs must be configured to use the same label distribution protocol. If there are multiple links connecting two LSRs, all of the link interfaces connecting the two LSRs must be configured to use the same protocol.

Examples

The following example shows how to establish LDP as the label distribution protocol for the interface:

```
Switch(config-if)# mpls label protocol ldp
```

mpls label range

To configure the range of local labels available for use with Multiprotocol Label Switching (MPLS) applications on packet interfaces, use the **mpls label range** command in global configuration mode. To revert to the platform defaults, use the **no** form of this command.

```
mpls label range minimum-value maximum-value [static minimum-static-value maximum-static-value]  
no mpls label range
```

Syntax Description	<i>minimum-value</i>	The value of the smallest label allowed in the label space. The default is 16.
	<i>maximum-value</i>	The value of the largest label allowed in the label space. The default is platform-dependent.
	static	(Optional) Reserves a block of local labels for static label assignments. If you omit the static keyword and the <i>minimum-static-value</i> <i>maximum-static-value</i> arguments, no labels are reserved for static assignment.
	<i>minimum-static-value</i>	(Optional) The minimum value for static label assignments. There is no default value.
	<i>maximum-static-value</i>	(Optional) The maximum value for static label assignments. There is no default value.

Command Default The platform's default values are used.

Command Modes

Global configuration

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

mpls label range**Usage Guidelines**

The labels 0 through 15 are reserved by the IETF (see RFC 3032, MPLS Label Stack Encoding, for details) and cannot be included in the range specified in the **mpls label range** command. If you enter a 0 in the command, you will get a message that indicates that the command is an unrecognized command.

The label range defined by the **mpls label range** command is used by all MPLS applications that allocate local labels (for dynamic label switching, MPLS traffic engineering, MPLS Virtual Private Networks (VPNs), and so on).

You can use label distribution protocols, such as Label Distribution Protocol (LDP), to reserve a generic range of labels from 16 through 1048575 for dynamic assignment.

You specify the optional **static** keyword, to reserve labels for static assignment. The MPLS Static Labels feature requires that you configure a range of labels for static assignment. You can configure static bindings only from the current static range. If the static range is not configured or is exhausted, then you cannot configure static bindings.

The range of label values is 16 to 4096. The maximum value defaults to 4096. You can split for static label space between say 16 to 100 and for dynamic label space between 101 to 4096.

The upper and lower minimum static label values are displayed in the help line. For example, if you configure the dynamic label with a minimum value of 16 and a maximum value of 100, the help lines display as follows:

```
Switch(config)# mpls label range 16 100 static ?
<100> Upper Minimum static label value
<16> Lower Minimum static label value
Reserved Label Range --> 0 to 15
Available Label Range --> 16 to 4096
Static Label Range --> 16 to 100
Dynamic Label Range --> 101 to 4096
```

In this example, you can configure a static range from 16 to 100.

If the lower minimum static label space is not available, the lower minimum is not displayed in the help line. For example:

```
Switch(config)# mpls label range 16 100 static ?
<16-100> static label value range
```

Examples

The following example shows how to configure the size of the local label space. In this example, the minimum static value is set to 200, and the maximum static value is set to 4000.

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# mpls label range 200 4000
Switch(config)#
```

If you had specified a new range that overlaps the current range (for example, the new range of the minimum static value set to 16 and the maximum static value set to 1000), then the new range takes effect immediately.

The following example show how to configure a dynamic local label space with a minimum static value set to 100 and the maximum static value set to 1000 and a static label space with a minimum static value set to 16 and a maximum static value set to 99:

```
Switch(config)# mpls label range 100 1000 static 16 99
Switch(config)#
```

In the following output, the **show mpls label range** command, executed after a reload, shows that the configured range is now in effect:

```
Switch# show mpls label range
Downstream label pool: Min/Max label: 100/1000
Range for static labels: Min/Max/Number: 16/99
```

The following example shows how to restore the label range to its default value:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# no mpls label range
Switch(config)# end
```

Related Commands

Command	Description
show mpls label range	Displays the range of the MPLS local label space.

mpls static binding ipv4

To bind a prefix to a local or remote label, use the **mpls static binding ipv4** command in global configuration mode. To remove the binding between the prefix and label, use the **no** form of this command.

```
mpls static binding ipv4 prefix mask {label | input label | output nexthop {explicit-null | implicit-nulllabel}}
no mpls static binding ipv4 prefix mask {label | input label | output nexthop {explicit-null | implicit-nulllabel}}
```

<i>prefix mask</i>	Specifies the prefix and mask to bind to a label. (When you do not use the input or output keyword, the specified label is an incoming label.) Note Without the arguments, the no form of the command removes all static bindings.
<i>label</i>	Binds a prefix or a mask to a local (incoming) label. (When you do not use the input or output keyword, the specified label is an incoming label.)
input <i>label</i>	Binds the specified label to the prefix and mask as a local (incoming) label.
output <i>nexthop explicit-null</i>	Binds the Internet Engineering Task Force (IETF) Multiprotocol Label Switching (MPLS) IPv4 explicit null label (0) as a remote (outgoing) label.
output <i>nexthop implicit-null</i>	Binds the IETF MPLS implicit null label (3) as a remote (outgoing) label.
output <i>nexthop label</i>	Binds the specified label to the prefix/mask as a remote (outgoing) label.

Command Default

Prefixes are not bound to local or remote labels.

Command Modes

Global configuration (config)

mpls static binding ipv4**Command History**

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines

The **mpls static binding ipv4** command pushes bindings into Label Distribution Protocol (LDP). LDP then needs to match the binding with a route in the Routing Information Base (RIB) or Forwarding Information Base (FIB) before installing forwarding information.

The **mpls static binding ipv4** command installs the specified bindings into the LDP Label Information Base (LIB). LDP will install the binding labels for forwarding use if or when the binding prefix or mask matches a known route.

Static label bindings are not supported for local prefixes, which are connected networks, summarized routes, default routes, and supernets. These prefixes use implicit-null or explicit-null as the local label.

If you do not specify the **input** or the **output** keyword, input (local label) is assumed.

For the **no** form of the command:

- If you specify the command name without any keywords or arguments, all static bindings are removed.
- Specifying the prefix and mask but no label parameters removes all static bindings for that prefix or mask.

Examples

In the following example, the **mpls static binding ipv4** command configures a static prefix and label binding before the label range is reconfigured to define a range for static assignment. The output of the command indicates that the binding has been accepted, but cannot be used for MPLS forwarding until you configure a range of labels for static assignment that includes that label.

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# mpls static binding ipv4 10.0.0.0 255.0.0.0 55
% Specified label 55 for 10.0.0.0/8 out of configured
% range for static labels. Cannot be used for forwarding until
% range is extended.
Router(config)# end
```

The following **mpls static binding ipv4** commands configure input and output labels for several prefixes:

```
Device(config)# mpls static binding ipv4 10.0.0.0 255.0.0.0 55
Device(config)# mpls static binding ipv4 10.0.0.0 255.0.0.0 output 10.0.0.66 2607
Device(config)# mpls static binding ipv4 10.66.0.0 255.255.0.0 input 17
Device(config)# mpls static binding ipv4 10.66.0.0 255.255.0.0 output 10.13.0.8 explicit-null
Device(config)# end
```

The following **show mpls static binding ipv4** command displays the configured bindings:

```
Device# show mpls static binding ipv4

10.0.0.0/8: Incoming label: 55
  Outgoing labels:
    10.0.0.66 2607
10.66.0.0/24: Incoming label: 17
  Outgoing labels:
    10.13.0.8   explicit-null
```

Related Commands	Command	Description
	show mpls forwarding-table	Displays labels currently being used for MPLS forwarding.
	show mpls label range	Displays statically configured label bindings.

show mpls forwarding-table

To display the contents of the Multiprotocol Label Switching (MPLS) Label Forwarding Information Base (LFIB), use the **show mpls forwarding-table** command in user EXEC or privileged EXEC mode.



Note When a local label is present, the forwarding entry for IP imposition will not be showed; if you want to see the IP imposition information, use **show ip cef**.

show mpls forwarding-table [{network {masklength} | interface interface | labels label [dash label] | lcatm atm atm-interface-number | next-hop address | lsp-tunnel [tunnel-id]}] [vrf vrf-name] [detail slot slot-number]

<i>network</i>	(Optional) Destination network number.
<i>mask</i>	IP address of the destination mask whose entry is to be shown.
<i>length</i>	Number of bits in the mask of the destination.
interface <i>interface</i>	(Optional) Displays entries with the outgoing interface specified.
labels <i>label-label</i>	(Optional) Displays entries with the local labels specified.
lcatm atm <i>atm-interface-number</i>	Displays ATM entries with the specified Label Controlled Asynchronous Transfer Mode (LCATM).
next-hop <i>address</i>	(Optional) Displays only entries with the specified neighbor as the next hop.
lsp-tunnel	(Optional) Displays only entries with the specified label switched path (LSP) tunnel, or with all LSP tunnel entries.
<i>tunnel-id</i>	(Optional) Specifies the LSP tunnel for which to display entries.
vrf <i>vrf-name</i>	(Optional) Displays entries with the specified VPN routing and forwarding (VRF) instance.
detail	(Optional) Displays information in long form (includes length of encapsulation, length of MAC string, maximum transmission unit [MTU], and all labels).
slot <i>slot-number</i>	(Optional) Specifies the slot number, which is always 0.

show mpls forwarding-table

Command Modes

User EXEC (>
Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced.

Examples

The following is sample output from the **show mpls forwarding-table** command:

```
Device# show mpls forwarding-table
Local Outgoing      Prefix          Bytes label Outgoing      Next Hop
Label Label or VC   or Tunnel Id   switched interface
26    No Label      10.253.0.0/16  0      Et4/0/0      10.27.32.4
28    1/33          10.15.0.0/16   0      AT0/0.1      point2point
29    Pop Label     10.91.0.0/16   0      Hs5/0        point2point
           1/36          10.91.0.0/16  0      AT0/0.1      point2point
30    32            10.250.0.97/32  0      Et4/0/2      10.92.0.7
           32            10.250.0.97/32  0      Hs5/0        point2point
34    26            10.77.0.0/24   0      Et4/0/2      10.92.0.7
           26            10.77.0.0/24   0      Hs5/0        point2point
35    No Label[T]   10.100.100.101/32 0      Tu301       point2point
36    Pop Label     10.1.0.0/16    0      Hs5/0        point2point
           1/37          10.1.0.0/16    0      AT0/0.1      point2point
[T]      Forwarding through a TSP tunnel.
View additional labeling info with the 'detail' option
```

The following is sample output from the **show mpls forwarding-table** command when the IPv6 Provider Edge Router over MPLS feature is configured to allow IPv6 traffic to be transported across an IPv4 MPLS backbone. The labels are aggregated because there are several prefixes for one local label, and the prefix column contains “IPv6” instead of a target prefix.

```
Device# show mpls forwarding-table
Local Outgoing      Prefix          Bytes label Outgoing      Next Hop
Label Label or VC   or Tunnel Id   switched interface
16    Aggregate     IPv6          0
17    Aggregate     IPv6          0
18    Aggregate     IPv6          0
19    Pop Label     192.168.99.64/30 0      Se0/0        point2point
20    Pop Label     192.168.99.70/32 0      Se0/0        point2point
21    Pop Label     192.168.99.200/32 0      Se0/0        point2point
22    Aggregate     IPv6          5424
23    Aggregate     IPv6          3576
24    Aggregate     IPv6          2600
```

The following is sample output from the **show mpls forwarding-table detail** command. If the MPLS EXP level is used as a selection criterion for packet forwarding, a bundle adjacency exp (vcd) field is included in the display. This field includes the EXP value and the corresponding virtual circuit descriptor (VCD) in parentheses. The line in the output that reads “No output feature configured” indicates that the MPLS egress NetFlow accounting feature is not enabled on the outgoing interface for this prefix.

```
Device# show mpls forwarding-table detail
Local Outgoing      Prefix          Bytes label Outgoing      Next Hop
label   label or VC   or Tunnel Id   switched interface
16    Pop label     10.0.0.6/32    0      AT1/0.1      point2point
```

```

        Bundle adjacency exp(vcd)
        0(1) 1(1) 2(1) 3(1) 4(1) 5(1) 6(1) 7(1)
        MAC/Encaps=12/12, MTU=4474, label Stack={}
          00010000AAAA030000008847
        No output feature configured
17    18           10.0.0.9/32      0       AT1/0.1      point2point
        Bundle adjacency exp(vcd)
        0(1) 1(1) 2(1) 3(1) 4(1) 5(1) 6(1) 7(1)
        MAC/Encaps=12/16, MTU=4470, label Stack{18}
          00010000AAAA030000008847 00012000
        No output feature configured
18    19           10.0.0.10/32     0       AT1/0.1     point2point
        Bundle adjacency exp(vcd)
        0(1) 1(1) 2(1) 3(1) 4(1) 5(1) 6(1) 7(1)
        MAC/Encaps=12/16, MTU=4470, label Stack{19}
          00010000AAAA030000008847 00013000
        No output feature configured
19    17           10.0.0.0/8       0       AT1/0.1     point2point
        Bundle adjacency exp(vcd)
        0(1) 1(1) 2(1) 3(1) 4(1) 5(1) 6(1) 7(1)
        MAC/Encaps=12/16, MTU=4470, label Stack{17}
          00010000AAAA030000008847 00011000
        No output feature configured
20    20           10.0.0.0/8       0       AT1/0.1     point2point
        Bundle adjacency exp(vcd)
        0(1) 1(1) 2(1) 3(1) 4(1) 5(1) 6(1) 7(1)
        MAC/Encaps=12/16, MTU=4470, label Stack{20}
          00010000AAAA030000008847 00014000
        No output feature configured
21    Pop label     10.0.0.0/24     0       AT1/0.1     point2point
        Bundle adjacency exp(vcd)
        0(1) 1(1) 2(1) 3(1) 4(1) 5(1) 6(1) 7(1)
        MAC/Encaps=12/12, MTU=4474, label Stack={}
          00010000AAAA030000008847
        No output feature configured
22    Pop label     10.0.0.4/32     0       Et2/3       10.0.0.4
        MAC/Encaps=14/14, MTU=1504, label Stack={}
          000427AD10430005DDFE043B8847
        No output feature configured

```

The following is sample output from the **show mpls forwarding-table detail** command. In this example, the MPLS egress NetFlow accounting feature is enabled on the first three prefixes, as indicated by the line in the output that reads “Feature Quick flag set.”

```

Device# show mpls forwarding-table detail
Local  Outgoing   Prefix          Bytes label  Outgoing   Next Hop
label   label or VC  or Tunnel Id  switched   interface
16     Aggregate  10.0.0.0/8[V]    0
      MAC/Encaps=0/0, MTU=0, label Stack={}
      VPN route: vpn1
      Feature Quick flag set
Per-packet load-sharing, slots: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
17     No label   10.0.0.0/8[V]    0       Et0/0/2   10.0.0.1
      MAC/Encaps=0/0, MTU=1500, label Stack={}
      VPN route: vpn1
      Feature Quick flag set
Per-packet load-sharing, slots: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
18     No label   10.42.42.42/32[V] 4185    Et0/0/2   10.0.0.1
      MAC/Encaps=0/0, MTU=1500, label Stack={}
      VPN route: vpn1
      Feature Quick flag set
Per-packet load-sharing, slots: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
19     2/33       10.41.41.41/32   0       AT1/0/0.1 point2point

```

show mpls forwarding-table

```
MAC/Encaps=4/8, MTU=4470, label Stack{2/33(vcd=2)}
00028847 00002000
No output feature configured
```

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

Table 94: show mpls forwarding-table Field Descriptions

Field	Description
Local label	Label assigned by this device.
Outgoing Label or VC Note This field is not supported on the Cisco 10000 series routers.	Label assigned by the next hop or the virtual path identifier (VPI)/virtual channel identifier (VCI) used to get to next hop. The entries in this column are the following: <ul style="list-style-type: none"> • [T]--Forwarding is through an LSP tunnel. • No Label--There is no label for the destination from the next hop or label switching is not enabled on the outgoing interface. • Pop Label--The next hop advertised an implicit NULL label for the destination and the device removed the top label. • Aggregate--There are several prefixes for one local label. This entry is used when IPv6 is configured on edge devices to transport IPv6 traffic over an IPv4 MPLS network.
Prefix or Tunnel Id	Address or tunnel to which packets with this label are sent. Note If IPv6 is configured on edge devices to transport IPv6 traffic over an IPv4 MPLS network, “IPv6” is displayed here. <ul style="list-style-type: none"> • [V]--The corresponding prefix is in a VRF.
Bytes label switched	Number of bytes switched with this incoming label. This includes the outgoing label and Layer 2 header.
Outgoing interface	Interface through which packets with this label are sent.
Next Hop	IP address of the neighbor that assigned the outgoing label.
Bundle adjacency exp(vcd)	Bundle adjacency information. Includes the MPLS EXP value and the corresponding VCD.
MAC/Encaps	Length in bytes of the Layer 2 header and length in bytes of the packet encapsulation, including the Layer 2 header and label header.
MTU	MTU of the labeled packet.
label Stack	All the outgoing labels. If the outgoing interface is transmission convergence (TC)-ATM, the VCD is also shown. Note TC-ATM is not supported on Cisco 10000 series routers.

Field	Description
00010000AAAA030000008847 00013000	The actual encapsulation in hexadecimal form. A space is shown between Layer 2 and the label header.

Explicit-Null Label Example

The following is sample output, including the explicit-null label = 0 (commented in bold), for the **show mpls forwarding-table** command on a CSC-PE device:

```
Device# show mpls forwarding-table
Local Outgoing Prefix Bytes label Outgoing Next Hop
label label or VC or Tunnel Id switched interface
17 Pop label 10.10.0.0/32 0 Et2/0 10.10.0.1
18 Pop label 10.10.10.0/24 0 Et2/0 10.10.0.1
19 Aggregate 10.10.20.0/24[V] 0
20 Pop label 10.10.200.1/32[V] 0 Et2/1 10.10.10.1
21 Aggregate 10.10.1.1/32[V] 0
22 0 192.168.101.101/32[V] \
      0 Et2/1 192.168.101.101
23 0 192.168.101.100/32[V] \
      0 Et2/1 192.168.101.100
25 0 192.168.102.125/32[V] 0 Et2/1 192.168.102.125 !outlabel
value 0
```

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

Table 95: show mpls forwarding-table Field Descriptions

Field	Description
Local label	Label assigned by this device.
Outgoing label or VC	<p>Label assigned by the next hop or VPI/VCI used to get to the next hop. The entries in this column are the following:</p> <ul style="list-style-type: none"> • [T]--Forwarding is through an LSP tunnel. • No label--There is no label for the destination from the next hop or that label switching is not enabled on the outgoing interface. • Pop label--The next hop advertised an implicit NULL label for the destination and that this device popped the top label. • Aggregate--There are several prefixes for one local label. This entry is used when IPv6 is configured on edge devices to transport IPv6 traffic over an IPv4 MPLS network. • 0--The explicit null label value = 0.
Prefix or Tunnel Id	<p>Address or tunnel to which packets with this label are sent.</p> <p>Note If IPv6 is configured on edge devices to transport IPv6 traffic over an IPv4 MPLS network, IPv6 is displayed here.</p> <ul style="list-style-type: none"> • [V]--Means that the corresponding prefix is in a VRF.

show mpls forwarding-table

Field	Description
Bytes label switched	Number of bytes switched with this incoming label. This includes the outgoing label and Layer 2 header.
Outgoing interface	Interface through which packets with this label are sent.
Next Hop	IP address of the neighbor that assigned the outgoing label.

Cisco IOS Software Modularity: MPLS Layer 3 VPNs Example

The following is sample output from the **show mpls forwarding-table** command:

```
Device# show mpls forwarding-table
Local      Outgoing    Prefix          Bytes Label   Outgoing     Next Hop
Label      Label       or Tunnel Id   Switched
16         Pop Label   IPv4 VRF[V]    62951000    aggregate/v1
17         [H] No Label 10.1.1.0/24   0           AT1/0/0.1 point2point
                  No Label 10.1.1.0/24   0           PO3/1/0 point2point
                  [T] No Label 10.1.1.0/24   0           Tu1 point2point
18         [HT] Pop Label 10.0.0.3/32  0           Tu1 point2point
19         [H] No Label 10.0.0.0/8    0           AT1/0/0.1 point2point
                  No Label 10.0.0.0/8    0           PO3/1/0 point2point
20         [H] No Label 10.0.0.0/8    0           AT1/0/0.1 point2point
                  No Label 10.0.0.0/8    0           PO3/1/0 point2point
21         [H] No Label 10.0.0.1/32   812         AT1/0/0.1 point2point
                  No Label 10.0.0.1/32   0           PO3/1/0 point2point
22         [H] No Label 10.1.14.0/24  0           AT1/0/0.1 point2point
                  No Label 10.1.14.0/24  0           PO3/1/0 point2point
23         [HT] 16        172.1.1.0/24[V] 0           Tu1 point2point
24         [HT] 24        10.0.0.1/32[V]  0           Tu1 point2point
25         [H] No Label 10.0.0.0/8[V]  0           AT1/1/0.1 point2point
26         [HT] 16        10.0.0.3/32[V]  0           Tu1 point2point
27         No Label   10.0.0.1/32[V]  0           AT1/1/0.1 point2point
[T]          Forwarding through a TSP tunnel.
[H]          View additional labelling info with the 'detail' option
[H]          Local label is being held down temporarily.
```

The table below describes the Local Label fields relating to the Cisco IOS Software Modularity: MPLS Layer 3 VPNs feature.

Table 96: show mpls forwarding-table Field Descriptions

Field	Description
Local Label	<p>Label assigned by this device.</p> <ul style="list-style-type: none"> [H]--Local labels are in holddown, which means that the application that requested the labels no longer needs them and stops advertising them to its labeling peers. <p>The label's forwarding-table entry is deleted after a short, application-specific time.</p> <p>If any application starts advertising a held-down label to its labeling peers, the label could come out of holddown.</p> <p>Note [H] is not shown if labels are held down globally.</p> <p>A label enters global holddown after a stateful switchover or a restart of certain processes in a Cisco IOS modularity environment.</p> <ul style="list-style-type: none"> [T]--The label is forwarded through an LSP tunnel. <p>Note Although [T] is still a property of the outgoing interface, it is shown in the Local Label column.</p> <ul style="list-style-type: none"> [HT]--Both conditions apply.

L2VPN Inter-AS Option B: Example

The following is sample output from the **show mpls forwarding-table interface** command. In this example, the pseudowire identifier (that is, 4096) is displayed in the Prefix or Tunnel Id column.

The **show mpls l2transport vc detail** command can be used to obtain more information about the specific pseudowire displayed.

```
Device# show mpls forwarding-table
Local      Outgoing      Prefix          Bytes Label      Outgoing      Next Hop
Label     Label        or Tunnel Id    Switched      interface
1011      No Label     12ckt(4096)       0            none         point2point
```

The table below describes the fields shown in the display.

Table 97: show mpls forwarding-table interface Field Descriptions

Field	Description
Local Label	Label assigned by this device.
Outgoing Label	Label assigned by the next hop or virtual path identifier (VPI)/virtual channel identifier (VCI) used to get to the next hop.
Prefix or Tunnel Id	Address or tunnel to which packets with this label are going.
Bytes Label Switched	Number of bytes switched with this incoming label. This includes the outgoing label and Layer 2 header.

show mpls label range

Field	Description
Outgoing interface	Interface through which packets with this label are sent.
Next Hop	IP address of the neighbor that assigned the outgoing label.

show mpls label range

To display the range of local labels available for use on packet interfaces, use the **show mpls label range** command in privileged EXEC mode.

show mpls label range

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

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

Usage Guidelines You can use the **mpls label range** command to configure a range for local labels that is different from the default range. The **show mpls label range** command displays both the label range currently in use and the label range that will be in use following the next switch reload.

Examples In the following example, the use of the **show mpls label range** command is shown before and after the **mpls label range** command is used to configure a label range that does not overlap the starting label range:

```
Switch# show mpls label range
Downstream label pool: Min/Max label: 16/100
Switch# configure terminal
Switch(config)# mpls label range 101 4000
Switch(config)# exit
Switch# show mpls label range
Downstream label pool: Min/Max label: 101/4000
```

Related Commands	Command	Description
	mpls label range	Configures a range of values for use as local labels.

show mpls static binding

To display Multiprotocol Label Switching (MPLS) static label bindings, use the **show mpls static binding** command in privileged EXEC mode.

show mpls static binding[{ipv4[{vrf *vrf-name*}]}[{prefix{mask-length} }][{local | remote}][{nexthop address}]]

Syntax Description	ipv4	(Optional) Displays IPv4 static label bindings.
	vrf <i>vrf-name</i>	(Optional) The static label bindings for a specified VPN routing and forwarding instance.
	prefix {mask-length / mask}	(Optional) Labels for a specific prefix.
	local	(Optional) Displays the incoming (local) static label bindings.
	remote	(Optional) Displays the outgoing (remote) static label bindings.
	nexthop <i>address</i>	(Optional) Displays the label bindings for prefixes with outgoing labels for which the specified next hop is to be displayed.

Command Modes

Privileged EXEC (#)

Command History**Command History**

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines

If you do not specify any optional arguments, the **show mpls static binding** command displays information about all static label bindings. Or the information can be limited to any of the following:

- Bindings for a specific prefix or mask
- Local (incoming) labels
- Remote (outgoing) labels
- Outgoing labels for a specific next hop router

Examples

In the following output, the **show mpls static binding ipv4** command with no optional arguments displays all static label bindings:

```
Device# show mpls static binding ipv4
10.0.0.0/8: Incoming label: none;
  Outgoing labels:
    10.13.0.8      explicit-null
10.0.0.0/8: Incoming label: 55 (in LIB)
  Outgoing labels:
    10.0.0.66      2607
10.66.0.0/16: Incoming label: 17 (in LIB)
  Outgoing labels: None
```

In the following output, the **show mpls static binding ipv4** command displays remote (outgoing) statically assigned labels only:

show mpls static crossconnect

```
Device# show mpls static binding ipv4 remote
10.0.0.0/8:
  Outgoing labels:
    10.13.0.8      explicit-null
10.0.0.0/8:
  Outgoing labels:
    10.0.0.66      2607
```

In the following output, the **show mpls static binding ipv4** command displays local (incoming) statically assigned labels only:

```
Device# show mpls static binding ipv4 local
10.0.0.0/8: Incoming label: 55 (in LIB)
10.66.0.0/16: Incoming label: 17 (in LIB)
```

In the following output, the **show mpls static binding ipv4** command displays statically assigned labels for prefix 10.0.0.0 / 8 only:

```
Device# show mpls static binding ipv4 10.0.0.0/8
10.0.0.0/8: Incoming label: 55 (in LIB)
  Outgoing labels:
    10.0.0.66      2607
```

In the following output, the **show mpls static binding ipv4** command displays prefixes with statically assigned outgoing labels for next hop 10.0.0.66:

```
Device# show mpls static binding ipv4 10.0.0.0 8 nexthop 10.0.0.66
10.0.0.0/8: Incoming label: 55 (in LIB)
  Outgoing labels:
    10.0.0.66      2607
```

The following output, the **show mpls static binding ipv4 vrf** command displays static label bindings for a VPN routing and forwarding instance vpn100:

```
Device# show mpls static binding ipv4 vrf vpn100
192.168.2.2/32: (vrf: vpn100) Incoming label: 100020
Outgoing labels: None
192.168.0.29/32: Incoming label: 100003 (in LIB)
Outgoing labels: None
```

Related Commands

Command	Description
mpls static binding ipv4	Binds an IPv4 prefix or mask to a local or remote label.

show mpls static crossconnect

To display statically configured Label Forwarding Information Database (LFIB) entries, use the **show mpls static crossconnect** command in privileged EXEC mode.

show mpls static crossconnect [low label [high label]]

Syntax Description

<i>low label high label</i>	(Optional) The statically configured LFIB entries.
-----------------------------	--

Command Modes

Privileged EXEC (#)

Command History**Command History****Release****Modification**

Cisco IOS XE Everest
16.6.1 This command was introduced.

Usage Guidelines

If you do not specify any label arguments, then all the configured static cross-connects are displayed.

Examples

The following sample output from the **show mpls static crossconnect** command shows the local and remote labels:

```
Device# show mpls static crossconnect
Local  Outgoing   Outgoing   Next Hop
label  label      interface
45     46         pos5/0    point2point
```

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

Table 98: show mpls static crossconnect Field Descriptions

Field	Description
Local label	Label assigned by this router.
Outgoing label	Label assigned by the next hop.
Outgoing interface	Interface through which packets with this label are sent.
Next Hop	IP address of the next hop router's interface that is connected to this router's outgoing interface.

Related Commands

Command	Description
mpls static crossconnect	Configures an LFIB entry for the specified incoming label and outgoing interface.

```
show mpls static crossconnect
```

Multicast VPN Commands

- [ip multicast-routing](#), on page 547
- [ip multicast mrinfo-filter](#), on page 548
- [mdt data](#), on page 549
- [mdt default](#), on page 550
- [mdt log-reuse](#), on page 551
- [show ip pim mdt bgp](#), on page 552
- [show ip pim mdt history](#), on page 553
- [show ip pim mdt receive](#), on page 554
- [show ip pim mdt send](#), on page 555

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 <i>vrf-name</i> argument.				
Command Default	IP multicast routing is disabled.				
Command Modes	Global configuration (config).				
Command History	<table border="1"><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>Cisco IOS XE Denali 16.3.2</td><td>This command was introduced.</td></tr></tbody></table>	Release	Modification	Cisco IOS XE Denali 16.3.2	This command was introduced.
Release	Modification				
Cisco IOS XE Denali 16.3.2	This command was introduced.				

Usage Guidelines When IP multicast routing is disabled, the Cisco IOS software does not forward any multicast packets.

ip multicast mrinfo-filter

Note For IP multicast, after enabling IP multicast routing, PIM must be configured on all interfaces. Disabling IP multicast routing does not remove PIM; PIM still must be explicitly removed from the interface configurations.

Examples

The following example shows how to enable IP multicast routing:

```
Switch(config)# ip multicast-routing
```

The following example shows how to enable IP multicast routing on a specific VRF:

```
Switch(config)#
ip multicast-routing vrf vrf1
```

The following example shows how to disable IP multicast routing:

```
Switch(config)#
no ip multicast-routing
```

The following example shows how to enable MDS in Cisco IOS XE Release 3.3S a specific VRF:

```
Switch(config)#
ip multicast-routing vrf vrf1
```

Related Commands

Command	Description
ip pim	Enables PIM on an interface.

ip multicast mrinfo-filter

To filter multicast router information (mrinfo) request packets, use the **ip multicast mrinfo-filter** command in global configuration mode. To remove the filter on mrinfo requests, use the **no** form of this command.

```
ip multicast [vrf vrf-name] mrinfo-filter access-list
no ip multicast [vrf vrf-name] mrinfo-filter
```

Syntax Description

vrf	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
<i>vrf-name</i>	(Optional) Name assigned to the VRF.
<i>access-list</i>	IP standard numbered or named access list that determines which networks or hosts can query the local multicast device with the mrinfo command.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.2	This command was introduced.

Usage Guidelines The **ip multicast mrinfo-filter** command filters the mrinfo request packets from all of the sources denied by the specified access list. That is, if the access list denies a source, that source's mrinfo requests are filtered. mrinfo requests from any sources permitted by the ACL are allowed to proceed.

Examples The following example shows how to filter mrinfo request packets from all hosts on network 192.168.1.1 while allowing requests from any other hosts:

```
ip multicast mrinfo-filter 51
access-list 51 deny 192.168.1.1
access list 51 permit any
```

Related Commands	Command	Description
	mrinfo	Queries a multicast device about which neighboring multicast devices are peering with it.

mdt data

To specify a range of addresses to be used in the data multicast distribution tree (MDT) pool, use the **mdt data** command in VRF configuration or VRF address family configuration mode. To disable this function, use the **no** form of this command.

```
mdt data threshold kb/s
no mdt data threshold kb/s
```

Syntax Description	threshold <i>kb/s</i>	(Optional) Defines the bandwidth threshold value in kilobits per second (kb/s). The range is from 1 to 4294967.
---------------------------	------------------------------	---

Command Default A data MDT pool is not configured.

Command Modes VRF address family configuration (config-vrf-af)
VRF configuration (config-vrf)

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.2	This command was introduced.

Usage Guidelines A data MDT can include a maximum of 256 multicast groups per MVPN. Multicast groups used to create the data MDT are dynamically chosen from a pool of configured IP addresses.

Use the **mdt data** command to specify a range of addresses to be used in the data MDT pool. The threshold is specified in kb/s. Using the optional **list** keyword and *access-list* argument, you can define the (S, G) MVPN

mdt default

entries to be used in a data MDT pool, which would further limit the creation of a data MDT pool to the particular (S, G) MVPN entries defined in the access list specified for the *access-list* argument.

You can access the **mdt default** command by using the **ip vrf** global configuration command. You can also access the **mdt default** command by using the **vrf definition** global configuration command followed by the **address-family ipv4**VRF configuration command.

Examples

The following example shows how to configure the range of group addresses for the MDT data pool. A threshold of 500 kb/s has been set, which means that if a multicast stream exceeds 1 kb/s, then a data MDT is created.

```
ip vrf vrf1
  rd 1000:1
  route-target export 10:27
  route-target import 10:27
  mdt default 236.1.1.1
  mdt data 228.0.0.0 0.0.0.127 threshold 500 list 101
!
.
.
.
!
ip pim ssm default
ip pim vrf vrf1 accept-rp auto-rp
!
```

Related Commands

Command	Description
mdt default	Configures a default MDT group for a VPN VRF.

mdt default

To configure a default multicast distribution tree (MDT) group for a Virtual Private Network (VPN) routing and forwarding (VRF) instance, use the **mdt default** command in VRF configuration or VRF address family configuration mode. To disable this function, use the **no** form of this command.

mdt default*group-address*
no mdt default*group-address*

Syntax Description

<i>group-address</i>	IP address of the default MDT group. This address serves as an identifier for the community in that provider edge (PE) devices configured with the same group address become members of the group, allowing them to receive packets sent by each other.
----------------------	---

Command Default

The command is disabled.

Command Modes

VRF address family configuration (config-vrf-af) VRF configuration (config-vrf)

Command History

Release	Modification
Cisco IOS XE Denali 16.3.2	This command was introduced.

Usage Guidelines

The default MDT group must be the same group configured on all PE devices that belong to the same VPN.

If Source Specific Multicast (SSM) is used as the protocol for the default MDT, the source IP address will be the address used to source the Border Gateway Protocol (BGP) sessions.

A tunnel interface is created as a result of this command. By default, the destination address of the tunnel header is the *group-address* argument.

You can access the **mdt default** command by using the **ip vrf** global configuration command. You can also access the **mdt default** command by using the **vrf definition** global configuration command followed by the **address-family ipv4** VRF configuration command.

Examples

In the following example, Protocol Independent Multicast (PIM) SSM is configured in the backbone. Therefore, the default and data MDT groups are configured within the SSM range of IP addresses. Inside the VPN, PIM sparse mode (PIM-SM) is configured and only Auto-RP announcements are accepted.

```
ip vrf vrf1
  rd 1000:1
  mdt default 236.1.1.1
  mdt data 228.0.0.0 0.0.0.127 threshold 50
  mdt data threshold 50
  route-target export 1000:1
  route-target import 1000:1
!
!
```

Related Commands

Command	Description
mdt data	Configures the multicast group address range for data MDT groups.

mdt log-reuse

To enable the recording of data multicast distribution tree (MDT) reuse, use the **mdt log-reuse** command in VRF configuration or in VRF address family configuration mode. To disable this function, use the **no** form of this command.

```
mdt log-reuse
no mdt log-reuse
```

Syntax Description

This command has no arguments or keywords.

Command Default

The command is disabled.

Command Modes

VRF address family configuration (config-vrf-af) VRF configuration (config-vrf)

Command History

Release	Modification
Cisco IOS XE Denali 16.3.2	This command was introduced.

show ip pim mdt bgp

Usage Guidelines

The **mdt log-reuse** command generates a syslog message whenever a data MDT is reused.

You can access the **mdt log-reuse** command by using the **ip vrf** global configuration command. You can also access the **mdt log-reuse** command by using the **vrf definition** global configuration command followed by the **address-family ipv4** VRF configuration command.

Examples

The following example shows how to enable MDT log reuse:

```
mdt log-reuse
```

Related Commands

Command	Description
mdt data	Configures the multicast group address range for data MDT groups.
mdt default	Configures a default MDT group for a VPN VRF.

show ip pim mdt bgp

To show details about the Border Gateway Protocol (BGP) advertisement of the route distinguisher (RD) for the multicast distribution tree (MDT) default group, use the **show ip pim mdt bgp** command in user EXEC or privileged EXEC mode.

show ip pim [vrf *vrf-name*] mdt bgp

Syntax Description

vrf <i>vrf-name</i>	(Optional) Displays information about the BGP advertisement of the RD for the MDT default group associated with Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the <i>vrf-name</i> argument.
----------------------------	---

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Denali 16.3.2	This command was introduced.

Usage Guidelines

Use this command to show detailed BGP advertisement of the RD for the MDT default group.

Examples

The following is sample output from the **show ip pim mdt bgp** command:

```
Device# show ip pim mdt bgp
MDT-default group 232.2.1.4
    rid:10.1.1.1 next_hop:10.1.1.1
```

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

Table 99: show ip pim mdt bgp Field Descriptions

Field	Description
MDT-default group	The MDT default groups that have been advertised to this router.
rid:10.1.1.1	The BGP router ID of the advertising router.
next_hop:10.1.1.1	The BGP next hop address that was contained in the advertisement.

show ip pim mdt history

To display information about the history of data multicast distribution tree (MDT) groups that have been reused, use the **show ip pim mdt history** command in privileged EXEC mode.

show ip pim vrf vrf-name mdt history interval minutes

Syntax Description	<table border="1"> <tr> <td>vrf <i>vrf-name</i></td><td>Displays the history of data MDT groups that have been reused for the Multicast VPN (MVPN) routing and forwarding (MVRF) instance specified for the <i>vrf-name</i> argument.</td></tr> <tr> <td>interval <i>minutes</i></td><td>Specifies the interval (in minutes) for which to display information about the history of data MDT groups that have been reused. The range is from 1 to 71512 minutes (7 weeks).</td></tr> </table>	vrf <i>vrf-name</i>	Displays the history of data MDT groups that have been reused for the Multicast VPN (MVPN) routing and forwarding (MVRF) instance specified for the <i>vrf-name</i> argument.	interval <i>minutes</i>	Specifies the interval (in minutes) for which to display information about the history of data MDT groups that have been reused. The range is from 1 to 71512 minutes (7 weeks).
vrf <i>vrf-name</i>	Displays the history of data MDT groups that have been reused for the Multicast VPN (MVPN) routing and forwarding (MVRF) instance specified for the <i>vrf-name</i> argument.				
interval <i>minutes</i>	Specifies the interval (in minutes) for which to display information about the history of data MDT groups that have been reused. The range is from 1 to 71512 minutes (7 weeks).				

Command Modes Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.2	This command was introduced.

Usage Guidelines The output of the **show ip pim mdt history** command displays the history of reused MDT data groups for the interval specified with the **interval** keyword and *minutes* argument. The interval is from the past to the present, that is, from the time specified for the *minutes* argument to the time at which the command is issued.

Examples The following is sample output from the **show ip pim mdt history** command:

```
Device# show ip pim vrf vrf1 mdt history interval 20
      MDT-data send history for VRF - vrf1 for the past 20 minutes
      MDT-data group          Number of reuse
        10.9.9.8                3
        10.9.9.9                2
```

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

Table 100: show ip pim mdt history Field Descriptions

Field	Description
MDT-data group	The MDT data group for which information is being shown.

show ip pim mdt receive

Field	Description
Number of reuse	The number of data MDTs that have been reused in this group.

show ip pim mdt receive

To display the data multicast distribution tree (MDT) group mappings received from other provider edge (PE) routers, use the **show ip pim mdt receive** command in privileged EXEC mode.

show ip pim vrf *vrf-name* mdt receive [detail]

Syntax Description	<table border="1"> <tr> <td>vrf <i>vrf-name</i></td><td>Displays the data MDT group mappings for the Multicast VPN (MVPN) routing and forwarding (MVRF) instance specified for the <i>vrf-name</i> argument.</td></tr> <tr> <td>detail</td><td>(Optional) Provides a detailed description of the data MDT advertisements received.</td></tr> </table>	vrf <i>vrf-name</i>	Displays the data MDT group mappings for the Multicast VPN (MVPN) routing and forwarding (MVRF) instance specified for the <i>vrf-name</i> argument.	detail	(Optional) Provides a detailed description of the data MDT advertisements received.
vrf <i>vrf-name</i>	Displays the data MDT group mappings for the Multicast VPN (MVPN) routing and forwarding (MVRF) instance specified for the <i>vrf-name</i> argument.				
detail	(Optional) Provides a detailed description of the data MDT advertisements received.				

Command Modes Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.2	This command was introduced.

Usage Guidelines When a router wants to switch over from the default MDT to a data MDT, it advertises the VRF source, the group pair, and the global multicast address over which the traffic will be sent. If the remote router wants to receive this data, then it will join this global address multicast group.

Examples

The following is sample output from the **show ip pim mdt receive** command using the **detail** keyword for further information:

```
Device# show ip pim vrf vpn8 mdt receive detail
Joined MDT-data groups for VRF:vpn8
group:172.16.8.0 source:10.0.0.100 ref_count:13
(10.101.8.10, 225.1.8.1), 1d13h/00:03:28/00:02:26, OIF count:1, flags:TY
(10.102.8.10, 225.1.8.1), 1d13h/00:03:28/00:02:27, OIF count:1, flags:TY
```

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

Table 101: show ip pim mdt receive Field Descriptions

Field	Description
group:172.16.8.0	Group that caused the data MDT to be built.
source:10.0.0.100	VRF source that caused the data MDT to be built.
ref_count:13	Number of (S, G) pairs that are reusing this data MDT.
OIF count:1	Number of interfaces out of which this multicast data is being forwarded.

Field	Description
flags:	<p>Information about the entry.</p> <ul style="list-style-type: none"> • A--candidate Multicast Source Discovery Protocol (MSDP) advertisement • B--bidirectional group • D--dense • C--connected • F--register flag • I--received source-specific host report • J--join shortest path source tree (SPT) • L--local • M--MSDP created entry • P--pruned • R--RP bit set • S--sparse • s--Source Specific Multicast (SSM) group • T--SPT bit set • X--proxy join timer running • U--URL Rendezvous Directory (URD) • Y--joined MDT data group • y--sending to MDT data group • Z--multicast tunnel

show ip pim mdt send

To display the data multicast distribution tree (MDT) groups in use, use the **show ip pim mdt send** command in privileged EXEC mode.

show ip pim vrf *vrf-name* mdt send

Syntax Description	vrf <i>vrf-name</i>	Displays the data MDT groups in use by the Multicast VPN (MVPN) routing and forwarding (MVRF) instance specified for the <i>vrf-name</i> argument.
--------------------	----------------------------	--

Command Modes Privileged EXEC

show ip pim mdt send

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.2	This command was introduced.

Usage Guidelines Use this command to show the data MDT groups in use by a specified MVRF.

Examples

The following is sample output from the **show ip pim mdt send** command:

```
Device# show ip pim vrf vpn8 mdt send
MDT-data send list for VRF:vpn8
  (source, group)          MDT-data group      ref_count
  (10.100.8.10, 225.1.8.1) 232.2.8.0          1
  (10.100.8.10, 225.1.8.2) 232.2.8.1          1
  (10.100.8.10, 225.1.8.3) 232.2.8.2          1
  (10.100.8.10, 225.1.8.4) 232.2.8.3          1
  (10.100.8.10, 225.1.8.5) 232.2.8.4          1
  (10.100.8.10, 225.1.8.6) 232.2.8.5          1
  (10.100.8.10, 225.1.8.7) 232.2.8.6          1
  (10.100.8.10, 225.1.8.8) 232.2.8.7          1
  (10.100.8.10, 225.1.8.9) 232.2.8.8          1
  (10.100.8.10, 225.1.8.10) 232.2.8.9         1
```

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

Table 102: show ip pim mdt send Field Descriptions

Field	Description
source, group	Source and group addresses that this router has switched over to data MDTs.
MDT-data group	Multicast address over which these data MDTs are being sent.
ref_count	Number of (S, G) pairs that are reusing this data MDT.



PART **IX**

Network Management

- [Encrypted Traffic Analytics, on page 559](#)
- [Network Management Commands, on page 565](#)
- [Flexible NetFlow Commands, on page 631](#)

Encrypted Traffic Analytics

- [et-analytics](#), on page 559
- [et-analytics enable](#), on page 560
- [inactive time](#), on page 560
- [ip flow-export destination](#), on page 561
- [show flow monitor etta-mon cache](#), on page 562
- [show platform software et-analytics](#), on page 562
- [show platform software fed switch active fmf et-analytics-flow-dump](#), on page 563

et-analytics

To enter the global et-analytics configuration mode, use the **et-analytics** command in the global configuration mode.

et-analytics

Syntax Description	et-analytics	Enter the global et-analytics configuration mode.				
Command Default	Disabled.					
Command Modes	Global configuration (config)					
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td><td>This command was introduced.</td></tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.	
Release	Modification					
Cisco IOS XE Everest 16.6.1	This command was introduced.					

Example:

The following example shows how to enter the et-analytics configuration mode:

```
Device>enable
Device#configure terminal
Device(config)# et-analytics
```

et-analytics enable

et-analytics enable

To enable et-analytics configuration on a particular interface, use the **et-analytics enable** command in the interface configuration mode. To disable et-analytics, use the **no** form of the command.

et-analytics enable
no et-analytics enable

Syntax Description	et-analytics enable	Enables et-analytics on a particular interface..				
Command Default	Disabled.					
Command Modes	Interface configuration (config-if)					
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.	
Release	Modification					
Cisco IOS XE Everest 16.6.1	This command was introduced.					

Example:

The following example shows how to enable et-analytics on interface GigabitEthernet1/0/2.:

```
Device>enable
Device#configure terminal
Device(config)# interface gi1/0/2
Device(config-if)# et-analytics enable
```

inactive time

To configure et-analytics inactive timer value, use the **inactive time seconds** command in the et-analytics configuration mode. To disable the timer settings, use the **no** form of the command.

inactive time seconds
no inactive time seconds

Syntax Description	inactive time	Configures the inactive timer value.
	<i>seconds</i>	Timer value in seconds. The range is from 1 to 604800 and the default value is 60 seconds.
Command Default	Disabled.	
Command Modes	et-analytics configuration (config-et-analytics)	

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Example:

The following example shows how to configure an inactive timer of 10 seconds:

```
Device>enable
Device#configure terminal
Device(config)# et-analytics
Device(config-et-analytics)# inactive time 10
```

ip flow-export destination

To configure the global collector destination IP address, use the **ip flow-export destination *ip_address port*** command in the et-analytics configuration mode. To remove the collector destination IP address, use the **no** form of the command.

```
ip flow-export destination ip_address port
no ip flow-export destination ip_address port
```

Syntax Description	ip flow-export destination	Configures the global collector destination IP address and port.
	<i>ip_address</i>	Destination IP address.
	<i>port</i>	Destination port.

Command Default Disabled.

Command Modes et-analytics configuration (config-et-analytics)

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Example:

The following example shows how to configure a flow-exporter destination IP address of 10.1.1.1 and port 2055:

```
Device>enable
Device#configure terminal
Device(config)# et-analytics
Device(config-et)# ip flow-export destination 10.1.1.1 2055
```

show flow monitor etta-mon cache

show flow monitor etta-mon cache

To display ETA monitor cache details, use the **show flow monitor etta-mon cache** command in privileged EXEC mode.

show flow monitor etta-mon cache

Command Default	None				
Command Modes	Privileged EXEC				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td><td>This command was introduced.</td></tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				

Example:

The following example shows how to display ETA flow monitor cache details:

```
Device>enable
Device#configure terminal
Device# show flow monitor etta-mon cache
Cache type: Normal (Platform cache)
Cache size: 10000
Current entries: 4
Flows added: 6
Flows aged: 2
- Inactive timeout ( 15 secs) 2
IPV4 DESTINATION ADDRESS: 15.15.15.35
IPV4 SOURCE ADDRESS: 72.163.128.140
IP PROTOCOL: 17
TRNS SOURCE PORT: 53
TRNS DESTINATION PORT: 12032
counter bytes long: 128
counter packets long: 1
timestamp abs first: 06:23:24.799
timestamp abs last: 06:23:24.799
interface input: Null
interface output: Null
```

show platform software et-analytics

To display et-analytics configuration, use the **show platform software et-analytics** command in privileged EXEC mode.

show platform software et-analytics {global | interfaces}

Syntax Description	global Displays global et-analytics configuration.
---------------------------	---

interfaces Displays interface et-analytics configuration.

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

Command Modes	Privileged EXEC
----------------------	-----------------

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Example:

The following example shows how to display global et-analytics configuration:

```
Device>enable
Device#configure terminal
Device# show platform software et-analytics global

ET-Analytics Global state
=====
All Interfaces : Off
IP Flow-record Destination: 10.126.71.20 : 2055
Inactive timer: 0
ET-Analytics interfaces
GigabitEthernet1/0/3
```

The following example shows how to display global et-analytics configuration:

```
Device>enable
Device#configure terminal
Device# show platform software et-analytics interfaces

ET-Analytics interfaces
GigabitEthernet1/0/3
```

show platform software fed switch active fnf et-analytics-flow-dump

To display interface et-analytics flow dump, use the **show platform software fed switch active fnf et-analytics-flow-dump** command in privileged EXEC mode.

show platform software fed switch active fnf et-analytics-flow-dump

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

Command Modes	Privileged EXEC
----------------------	-----------------

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

```
■ show platform software fed switch active fnf et-analytics-flow-dump
```

Example:

The following example shows how to display interface et-analytics flow dump.:

```
Device>enable
Device#configure terminal
Device# show platform software fed switch active fnf et-analytics-flow-dump

ET Analytics Flow dump
=====
Total packets received (27)
Excess packets received (0)
(Index:0) 72.163.128.140, 15.15.15.35, protocol=17, source port=53, dest port=12032, flow
done=u
SPLT: len = 2, value = (25600,0)(128,0)
IDP: len = 128, value = 45:0:0:80:f0:6c:0:0:f9:11:
(Index:1) 72.163.128.140, 15.15.15.35, protocol=17, source port=53, dest port=32356, flow
done=u
SPLT: len = 2, value = (59649,0)(128,0)
IDP: len = 517, value = 45:0:2:5:c3:1:0:0:f9:11:
(Index:2) 15.15.15.35, 72.163.128.140, protocol=17, source port=12032, dest port=53, flow
done=u
SPLT: len = 2, value = (10496,0)(128,0)
IDP: len = 69, value = 45:0:0:45:62:ae:40:0:40:11:
(Index:3) 15.15.15.35, 72.163.128.140, protocol=17, source port=32356, dest port=53, flow
done=u
SPLT: len = 2, value = (10496,0)(128,0)
IDP: len = 69, value = 45:0:0:45:62:ad:40:0:40:11:
```

Network Management Commands

- [description \(ERSPAN\)](#), on page 566
- [destination \(ERSPAN\)](#), on page 567
- [erspan-id](#), on page 568
- [event manager applet](#), on page 569
- [filter \(ERSPAN\)](#), on page 572
- [ip ttl \(ERSPAN\)](#), on page 573
- [ip wccp](#), on page 574
- [monitor capture \(interface/control plane\)](#), on page 575
- [monitor capture buffer](#), on page 577
- [monitor capture clear](#), on page 578
- [monitor capture export](#), on page 578
- [monitor capture file](#), on page 579
- [monitor capture limit](#), on page 580
- [monitor capture match](#), on page 581
- [monitor capture start](#), on page 582
- [monitor capture stop](#), on page 582
- [monitor session](#), on page 583
- [monitor session destination](#), on page 584
- [monitor session filter](#), on page 588
- [monitor session source](#), on page 589
- [monitor session type erspan-source](#), on page 591
- [origin](#), on page 592
- [show ip sla statistics](#), on page 593
- [show capability feature monitor](#), on page 594
- [show monitor](#), on page 595
- [show monitor capture](#), on page 597
- [show monitor session](#), on page 598
- [show platform software fed switch ip wccp](#), on page 600
- [show platform software swspan](#), on page 602
- [snmp ifmib ifindex persist](#), on page 603
- [snmp-server enable traps](#), on page 604
- [snmp-server enable traps bridge](#), on page 606
- [snmp-server enable traps bulkstat](#), on page 607

description (ERSPAN)

- [snmp-server enable traps call-home, on page 608](#)
- [snmp-server enable traps cef, on page 609](#)
- [snmp-server enable traps cpu, on page 609](#)
- [snmp-server enable traps envmon, on page 610](#)
- [snmp-server enable traps errdisable, on page 611](#)
- [snmp-server enable traps flash, on page 612](#)
- [snmp-server enable traps isis, on page 613](#)
- [snmp-server enable traps license, on page 613](#)
- [snmp-server enable traps mac-notification, on page 614](#)
- [snmp-server enable traps ospf, on page 615](#)
- [snmp-server enable traps pim, on page 616](#)
- [snmp-server enable traps port-security, on page 617](#)
- [snmp-server enable traps power-ethernet, on page 618](#)
- [snmp-server enable traps snmp, on page 618](#)
- [snmp-server enable traps storm-control, on page 619](#)
- [snmp-server enable traps stpx, on page 620](#)
- [snmp-server enable traps transceiver, on page 621](#)
- [snmp-server enable traps vrfmib, on page 621](#)
- [snmp-server enable traps vstack, on page 622](#)
- [snmp-server engineID, on page 623](#)
- [snmp-server host, on page 624](#)
- [source \(ERSPAN\), on page 628](#)
- [switchport mode access, on page 629](#)
- [switchport voice vlan, on page 629](#)

description (ERSPAN)

To describe an Encapsulated Remote Switched Port Analyzer (ERSPAN) source session, use the **description** command in ERSPAN monitor source session configuration mode. To remove a description, use the **no** form of this command.

description *description*
no **description**

Syntax Description *description* Describes the properties for this session.

Command Default Description is not configured.

Command Modes ERSPAN monitor source session configuration mode (config-mon-erspan-src)

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines The *description* argument can be up to 240 characters.

Examples

The following example shows how to describe an ERSPAN source session:

```
Device(config)# monitor session 2 type erspan-source
Device(config-mon-erspan-src)# description source1
```

Related Commands

Command	Description
monitor session type	Configures a local ERSPAN source or destination session.

destination (ERSPAN)

To configure an Encapsulated Remote Switched Port Analyzer (ERSPAN) source session destination and specify destination properties, use the **destination** command in ERSPAN monitor source session configuration mode. To remove a destination session, use the **no** form of this command.

destination
no destination

Syntax Description

This command has no arguments or keywords.

Command Default

A source session destination is not configured.

Command Modes

ERSPAN monitor source session configuration mode (config-mon-erspan-src)

Command History

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

Usage Guidelines

ERSPAN traffic is GRE-encapsulated SPAN traffic that can only be processed by an ERSPAN destination session.

All ERSPAN source session (maximum 8) destination IP address need not be same. Enter the **ip address** command to configure the IP address for the ERSPAN destination sessions.

The ERSPAN source session destination IP address, which is configured on an interface on the destination switch, is the source of traffic that an ERSPAN destination session sends to destination ports. Configure the same address in both the source and destination sessions with the **ip address** command.

Examples

The following example shows how to configure an ERSPAN source session destination and enter the ERSPAN monitor destination session configuration mode to specify the destination properties:

```
Switch(config)# monitor session 2 type erspan-source
Switch(config-mon-erspan-src)# destination
Switch(config-mon-erspan-src-dst)#ip address 10.1.1.1
Switch(config-mon-erspan-src-dst) #
```

The following sample output from the **show monitor session all** displays different IP addresses for source session destinations:

erspan-id

```

Switch# show monitor session all

Session 1
-----
Type : ERSPAN Source Session
Status : Admin Disabled
Description : session1
Destination IP Address : 10.1.1.1

Session 2
-----
Type : ERSPAN Source Session
Status : Admin Disabled
Description : session2
Destination IP Address : 192.0.2.1

Session 3
-----
Type : ERSPAN Source Session
Status : Admin Disabled
Description : session3
Destination IP Address : 198.51.100.1

Session 4
-----
Type : ERSPAN Source Session
Status : Admin Disabled
Description : session4
Destination IP Address : 203.0.113.1

Session 5
-----
Type : ERSPAN Source Session
Status : Admin Disabled
Description : session5
Destination IP Address : 209.165.200.225

```

Related Commands

Command	Description
erspan-id	Configures the ID used by the destination session to identify the ERSPAN traffic.
ip ttl	Configures TTL values for packets in the ERSPAN traffic.
monitor session type erspan-source	Configures a local ERSPAN source session.
origin	Configures an IP address used as the source of the ERSPAN traffic.

erspan-id

To configure the ID used by the destination session to identify the Encapsulated Remote Switched Port Analyzer (ERSPAN) traffic, use the **erspan-id** command in ERSPAN monitor destination session configuration mode. To remove the configuration, use the **no** form of this command.

erspan-id *erspan-ID*
no erspan-id *erspan-ID*

Syntax Description	<i>erspan-id</i> ERSPAN ID used by the destination session. Valid values are from 1 to 1023.				
Command Default	ERSPAN IDs for destination sessions are not configured.				
Command Modes	ERSPAN monitor destination session configuration mode (config-mon-erspan-src-dst)				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				

Examples	The following example shows how to configure an ERSPAN ID for a destination session:
	<pre>Device(config)# monitor session 2 type erspan-source Device(config-mon-erspan-src)# destination Device(config-mon-erspan-src-dst)# erspan-id 3</pre>

Related Commands	Command	Description
	destination	Configures an ERSPAN destination session and specifies destination properties.
	monitor session type	Configures a local ERSPAN source or destination session.

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	<table border="1"> <tr> <td><i>applet-name</i></td><td>Name of the applet file.</td></tr> <tr> <td>authorization</td><td>(Optional) Specifies AAA authorization type for applet.</td></tr> <tr> <td>bypass</td><td>(Optional) Specifies EEM AAA authorization type bypass.</td></tr> <tr> <td>class</td><td>(Optional) Specifies the EEM policy class.</td></tr> </table>	<i>applet-name</i>	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.
<i>applet-name</i>	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.								

<i>class-options</i>	(Optional) The EEM policy class. You can specify either one of the following: <ul style="list-style-type: none">• <i>class-letter</i>-- Letter from A to Z that identifies each policy class. You can specify any one <i>class-letter</i>.• 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 Everest 16.6.1	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
```

filter (ERSPAN)

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.

filter (ERSPAN)

To configure the Encapsulated Remote Switched Port Analyzer (ERSPAN) source VLAN filtering when the ERSPAN source is a trunk port, use the **filter** command in ERSPAN monitor source session configuration mode. To remove the configuration, use the **no** form of this command.

```
filter {ip access-group {standard-access-list extended-access-list acl-name} | ipv6 access-group acl-name
| mac access-group acl-name | vlan vlan-id [{,}] [-]}
no filter {ip [{access-group} | [{standard-access-list extended-access-list acl-name}]] | ipv6
[{access-group}] | mac [{access-group}] | vlan vlan-id [{,}] [-]}
```

Syntax Description	ip	Specifies the IP access control rules.
	access-group	Specifies an access control group.
	<i>standard-access-list</i>	Standard IP access list.
	<i>extended-access-list</i>	Extended IP access list.
	<i>acl-name</i>	Access list name.
	ipv6	Specifies the IPv6 access control rules.
	mac	Specifies the media access control (MAC) rules.
	vlan <i>vlan-ID</i>	Specifies the ERSPAN source VLAN. Valid values are from 1 to 4094.
	,	(Optional) Specifies another VLAN.
	-	(Optional) Specifies a range of VLANs.

Command Default	Source VLAN filtering is not configured.				
Command Modes	ERSPAN monitor source session configuration mode (config-mon-erspan-src)				
Command History	<table border="1"> <thead> <tr> <th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td>Cisco IOS XE Denali 16.3.1</td><td>This command was introduced.</td></tr> </tbody> </table>	Release	Modification	Cisco IOS XE Denali 16.3.1	This command was introduced.
Release	Modification				
Cisco IOS XE Denali 16.3.1	This command was introduced.				
Usage Guidelines	<p>You cannot include source VLANs and filter VLANs in the same session.</p> <p>When you configure the filter command on a monitored trunk interface, only traffic on that set of specified VLANs is monitored.</p>				
Examples	The following example shows how to configure source VLAN filtering:				
	<pre>Device(config)# monitor session 2 type erspan-source Device(config-mon-erspan-src)# filter vlan 3</pre>				
Related Commands	<table border="1"> <thead> <tr> <th>Command</th><th>Description</th></tr> </thead> <tbody> <tr> <td>monitor session type erspan-source</td><td>Configures a local ERSPAN source session.</td></tr> </tbody> </table>	Command	Description	monitor session type erspan-source	Configures a local ERSPAN source session.
Command	Description				
monitor session type erspan-source	Configures a local ERSPAN source session.				

ip ttl (ERSPAN)

To configure Time to Live (TTL) values for packets in the Encapsulated Remote Switched Port Analyzer (ERSPAN) traffic, use the **ip ttl** command in ERSPAN monitor destination session configuration mode. To remove the TTL values, use the **no** form of this command.

ip ttl *ttl-value*
no ip ttl *ttl-value*

Syntax Description	<i>ttl-value</i> TTL value. Valid values are from 2 to 255.				
Command Default	TTL value is set as 255.				
Command Modes	ERSPAN monitor destination session configuration mode (config-mon-erspan-src-dst)				
Command History	<table border="1"> <thead> <tr> <th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td><td>This command was introduced.</td></tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				

Examples The following example shows how to configure TTL value for ERSPAN traffic:

```
Device(config)# monitor session 2 type erspan-source
Device(config-mon-erspan-src)# destination
```

```
Device(config-mon-erspan-src-dst)# ip ttl 32
```

Related Commands

Command	Description
destination	Configures an ERSPAN destination session and specifies destination properties.
monitor session type	Configures a local ERSPAN source or destination session.

ip wccp

To enable the web cache service, and specify the service number that corresponds to a dynamic service that is defined by the application engine, use the **ip wccp** global configuration command on the device. Use the **no** form of this command to disable the service.

```
ip wccp {web-cache | service-number} [group-address groupaddress] [group-list access-list]
[redirect-list access-list] [password encryption-number password]
no ip wccp {web-cache | service-number} [group-address groupaddress] [group-list access-list]
[redirect-list access-list] [password encryption-number password]
```

Syntax Description

web-cache	Specifies the web-cache service (WCCP Version 1 and Version 2).
<i>service-number</i>	Dynamic service identifier, which means the service definition is dictated by the cache. The dynamic service number can be from 0 to 254. The maximum number of services is 256, which includes the web-cache service specified with the web-cache keyword.
group-address groupaddress	(Optional) Specifies the multicast group address used by the devices and the application engines to participate in the service group.
group-list access-list	(Optional) If a multicast group address is not used, specifies a list of valid IP addresses that correspond to the application engines that are participating in the service group.
redirect-list access-list	(Optional) Specifies the redirect service for specific hosts or specific packets from hosts.
password encryption-number password	(Optional) Specifies an encryption number. The range is 0 to 7. Use 0 for not encrypted, and use 7 for proprietary. Also, specifies a password name up to seven characters in length. The device combines the password with the MD5 authentication value to create security for the connection between the device and the application engine. By default, no password is configured, and no authentication is performed.

Command Default

WCCP services are not enabled on the device.

Command Modes

Global configuration

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines WCCP transparent caching bypasses Network Address Translation (NAT) when Cisco Express Forwarding switching is enabled. To work around this situation, configure WCCP transparent caching in the outgoing direction, enable Cisco Express Forwarding switching on the content engine interface, and specify the **ip wccp web-cache redirect out** command. Configure WCCP in the incoming direction on the inside interface by specifying the **ip wccp redirect exclude in** command on the router interface facing the cache. This configuration prevents the redirection of any packets arriving on that interface.

You can also include a redirect list when configuring a service group. The specified redirect list will deny packets with a NAT (source) IP address and prevent redirection.

This command instructs a device to enable or disable support for the specified service number or the web-cache service name. A service number can be from 0 to 254. Once the service number or name is enabled, the router can participate in the establishment of a service group.

When the **no ip wccp** command is entered, the device terminates participation in the service group, deallocates space if none of the interfaces still have the service configured, and terminates the WCCP task if no other services are configured.

The keywords following the **web-cache** keyword and the *service-number* argument are optional and may be specified in any order, but only may be specified once.

Example

The following example configures a web cache, the interface connected to the application engine or the server, and the interface connected to the client:

```
Device(config)# ip wccp web-cache
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# no switchport
Device(config-if)# ip address 172.20.10.30 255.255.255.0
Device(config-if)# no shutdown
Device(config-if)# exit
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# no switchport
Device(config-if)#
*Dec  6 13:11:29.507: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/3, changed state to down

Device(config-if)# ip address 175.20.20.10 255.255.255.0
Device(config-if)# no shutdown
Device(config-if)# ip wccp web-cache redirect in
Device(config-if)# ip wccp web-cache group-listen
Device(config-if)# exit
```

monitor capture (interface/control plane)

To configure monitor capture points specifying an attachment point and the packet flow direction or add more attachment points to a capture point, use the **monitor capture** command in privileged EXEC mode. To disable the monitor capture with the specified attachment point and the packet flow direction or disable one of multiple attachment points on a capture point, use the **no** form of this command.

monitor capture (interface/control plane)

```
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	<p>capture-name The name of the capture to be defined.</p> <p>interface interface-type interface-id Specifies an interface with <i>interface-type</i> and <i>interface-id</i> as an attachment point. The arguments have these meanings:</p> <ul style="list-style-type: none"> control-plane Specifies the control plane as an attachment point. in out both Specifies the traffic direction to be captured. 				
Command Default	A Wireshark capture is not configured.				
Command Modes	Privileged EXEC				
Command History	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; padding-bottom: 5px;">Release</th><th style="text-align: left; padding-bottom: 5px;">Modification</th></tr> </thead> <tbody> <tr> <td></td><td style="padding-top: 5px;">This command was introduced.</td></tr> </tbody> </table>	Release	Modification		This command was introduced.
Release	Modification				
	This command was introduced.				
Usage Guidelines	<p>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.</p> <p>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.</p> <p>Multiple attachment points can be associated with a capture point by re-running this command with another attachment point. An example is provided below.</p> <p>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.).</p> <p>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.</p> <p>Neither VRFs, management ports, nor private VLANs can be used as attachment points.</p> <p>Wireshark cannot capture packets on a destination SPAN port.</p> <p>When a VLAN is used as a Wireshark attachment point, packets are captured in the input direction only.</p>				

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

This command was introduced.

Usage Guidelines

When you first configure a Wireshark capture, a circular buffer of a small size is suggested.

monitor capture clear**Example**

To configure a circular buffer with a size of 1 MB:

```
Device# monitor capture mycap buffer circular size 1
```

monitor capture clear

To clear the monitor capture (Wireshark) buffer, use the **monitor capture clear** command in privileged EXEC mode.

monitor capture {capture-name} clear

Syntax Description

capture-name The name of the capture whose buffer is to be cleared.

Command Default

The buffer content is not cleared.

Command Modes

Privileged EXEC

Command History**Release****Modification**

This command was introduced.

Usage Guidelines

Use the **monitor capture clear** command either during capture or after the capture has stopped either because one or more end conditions has been met, or you entered the **monitor capture stop** command. If you enter the **monitor capture clear** command after the capture has stopped, the **monitor capture export** command that is used to store the contents of the captured packets in a file will have no impact because the buffer has no captured packets.

If you have more than one capture that is storing packets in a buffer, clear the buffer before starting a new capture to avoid memory loss.

Example

To clear the buffer contents for capture mycap:

```
Device# monitor capture mycap clear
```

monitor capture export

To export a monitor capture (Wireshark) to a file, use the **monitor capture export** command in privileged EXEC mode.

monitor capture {capture-name} export file-location : file-name

Syntax Description

capture-name The name of the capture to be exported.

file-location : file-name (Optional) Specifies the location and file name of the capture storage file.
Acceptable values for *file-location*:

- flash—On-board flash storage
 - — 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 file

To configure monitor capture (Wireshark) storage file attributes, use the **monitor capture file** command in privileged EXEC mode. To remove a storage file attribute, use the **no** form of this command.

```
monitor capture {capture-name} file{ [ buffer-size temp-buffer-size ] [ location file-location : file-name ] [ ring number-of-ring-files ] [ size total-size ] }
no monitor capture {capture-name} file{ [ buffer-size ] [ location ] [ ring ] [ size ] }
```

Syntax Description *capture-name* The name of the capture to be modified.

buffer-size *temp-buffer-size* (Optional) Specifies the size of the temporary buffer. The range for *temp-buffer-size* is 1 to 100 MB. This is specified to reduce packet loss.

monitor capture limit

location *file-location : file-name* (Optional) Specifies the location and file name of the capture storage file. Acceptable values for *file-location*:

- flash—On-board flash storage
- — USB drive

ring *number-of-ring-files* (Optional) Specifies that the capture is to be stored in a circular file chain and the number of files in the file ring.

size *total-size* (Optional) Specifies the total size of the capture files.

Command Default None

Command Modes Privileged EXEC

Command History	Release	Modification
		This command was introduced.

Usage Guidelines Use the **monitor capture file** command only when the storage destination is a file. The file may be stored either remotely or locally. Use this command after the packet capture has stopped. The packet capture is stopped when one or more end conditions have been met or you entered the **monitor capture stop** command.

When Wireshark is used on switches in a stack, packet captures can be stored only on the devices specified for *file-location* above that are connected to the active switch. Example: flash1 is connected to the active switch. flash2 is connected to the secondary switch. Only flash1 can be used to store packet captures.



Note Attempts to store packet captures on unsupported devices or devices not connected to the active switch will probably result in errors.

Example

To specify that the storage file name is mycap.pcap, stored on a flash drive:

```
Device# monitor capture mycap file location flash:mycap.pcap
```

monitor capture limit

To configure capture limits, use the **monitor capture limit** command in privileged EXEC mode. To remove the capture limits, use the **no** form of this command.

```
monitor capture {capture-name} limit {[duration seconds] [packet-length size] [packets num]}
no monitor capture {capture-name} limit [duration] [packet-length] [packets]
```

Syntax Description *capture-name* The name of the capture to be assigned capture limits.

duration <i>seconds</i>	(Optional) Specifies the duration of the capture, in seconds. The range is from 1 to 1000000.				
packet-length <i>size</i>	(Optional) Specifies the packet length, in bytes. If the actual packet is longer than the specified length, only the first set of bytes whose number is denoted by the bytes argument is stored.				
packets <i>num</i>	(Optional) Specifies the number of packets to be processed for capture.				
Command Default	Capture limits are not configured.				
Command Modes	Privileged EXEC				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td></td> <td>This command was introduced.</td></tr> </tbody> </table>	Release	Modification		This command was introduced.
Release	Modification				
	This command was introduced.				

Example

To configure a session limit of 60 seconds and a packet segment length of 400 bytes:

```
Device# monitor capture mycap limit duration 60 packet-len 400
```

monitor capture match

To define an explicit inline core filter for a monitor (Wireshark) capture, use the **monitor capture match** command in privileged EXEC mode. To remove this filter, use the **no** form of this command.

```
monitor capture {capture-name} match {any | mac mac-match-string | ipv4 {any | host | protocol} {any | host} | ipv6 {any | host | protocol} {any | host}}  
no monitor capture {capture-name} match
```

Syntax Description	<table border="1"> <tr> <td><i>capture-name</i></td><td>The name of the capture to be assigned a core filter.</td></tr> <tr> <td>any</td><td>Specifies all packets.</td></tr> <tr> <td>mac <i>mac-match-string</i></td><td>Specifies a Layer 2 packet.</td></tr> <tr> <td>ipv4</td><td>Specifies IPv4 packets.</td></tr> <tr> <td>host</td><td>Specifies the host.</td></tr> <tr> <td>protocol</td><td>Specifies the protocol.</td></tr> <tr> <td>ipv6</td><td>Specifies IPv6 packets.</td></tr> </table>	<i>capture-name</i>	The name of the capture to be assigned a core filter.	any	Specifies all packets.	mac <i>mac-match-string</i>	Specifies a Layer 2 packet.	ipv4	Specifies IPv4 packets.	host	Specifies the host.	protocol	Specifies the protocol.	ipv6	Specifies IPv6 packets.
<i>capture-name</i>	The name of the capture to be assigned a core filter.														
any	Specifies all packets.														
mac <i>mac-match-string</i>	Specifies a Layer 2 packet.														
ipv4	Specifies IPv4 packets.														
host	Specifies the host.														
protocol	Specifies the protocol.														
ipv6	Specifies IPv6 packets.														

Command Default	A core filter is not configured.
------------------------	----------------------------------

Command Modes	Privileged EXEC
----------------------	-----------------

monitor capture start

Command History	Release	Modification
		This command was introduced.

Examples

To define a capture point and the core filter for the capture point that matches to any IP version 4 packets on the source or destination:

```
Device# monitor capture mycap interface GigabitEthernet1/0/1 in
Device# monitor capture mycap match ipv4 any any
```

monitor capture start

To start the capture of packet data at a traffic trace point into a buffer, use the **monitor capture start** command in privileged EXEC mode.

monitor capture {capture-name} start

Syntax Description	<i>capture-name</i> The name of the capture to be started.	
Command Default	The buffer content is not cleared.	
Command Modes	Privileged EXEC	
Command History	Release	Modification
		This command was introduced.

Usage Guidelines	Use the monitor capture clear command to enable the packet data capture after the capture point is defined. To stop the capture of packet data, use the monitor capture stop command.
	Ensure that system resources such as CPU and memory are available before starting a capture.

Example

To start capturing buffer contents:

```
Device# monitor capture mycap start
```

monitor capture stop

To stop the capture of packet data at a traffic trace point, use the **monitor capture stop** command in privileged EXEC mode.

monitor capture {capture-name} stop

Syntax Description	<i>capture-name</i> The name of the capture to be stopped.	
Command Default	The packet data capture is ongoing.	
Command Modes	Privileged EXEC	
Command History	Release	Modification
		This command was introduced.
Usage Guidelines	Use the monitor capture stop command to stop the capture of packet data that you started using the monitor capture start command. You can configure two types of capture buffers: linear and circular. When the linear buffer is full, data capture stops automatically. When the circular buffer is full, data capture starts from the beginning and the data is overwritten.	

Example

To stop capturing buffer contents:

```
Device# monitor capture mycap stop
```

monitor session

To create a new Ethernet Switched Port Analyzer (SPAN) or a Remote Switched Port Analyzer (RSPAN) session configuration for analyzing traffic between ports or add to an existing session configuration, use the **monitor session** global configuration command. To clear SPAN or RSPAN sessions, use the **no** form of this command.

```
monitor session session-number {destination | filter | source}
no monitor session {session-number [destination | filter | source] | all | local | range
session-range | remote}
```

Syntax Description	<i>session-number</i>
all	Clears all monitor sessions.
local	Clears all local monitor sessions.
range <i>session-range</i>	Clears monitor sessions in the specified range.
remote	Clears all remote monitor sessions.
Command Default	No monitor sessions are configured.
Command Modes	Global configuration

monitor session destination

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines	You can verify your settings by entering the show monitor privileged EXEC command. You can display SPAN, RSPAN, FSPAN, and FRSPAN configuration on the switch by entering the show running-config privileged EXEC command. SPAN information appears near the end of the output.
-------------------------	---

Example

This example shows how to create a local SPAN session 1 to monitor traffic on Po13 (an EtherChannel port) and limit SPAN traffic in the session only to VLAN 1281. Egress traffic replicates the source; ingress forwarding is not enabled.

```
Device(config)# monitor session 1 source interface Po13
Device(config)# monitor session 1 filter vlan 1281
Device(config)# monitor session 1 destination interface GigabitEthernet2/0/36 encapsulation
  replicate
Device(config)# monitor session 1 destination interface GigabitEthernet3/0/36 encapsulation
  replicate
```

The following is the output of a **show monitor session all** command after completing these setup instructions:

```
Device# show monitor session all

Session 1
-----
Type          : Local Session
Source Ports  :
  Both        : Po13
Destination Ports   : Gi2/0/36, Gi3/0/36
  Encapsulation : Replicate
    Ingress    : Disabled
  Filter VLANs : 1281
  ...
  ...
```

monitor session destination

To start a new Switched Port Analyzer (SPAN) session or Remote SPAN (RSPAN) destination session, to enable ingress traffic on the destination port for a network security device (such as a Cisco IDS Sensor Appliance), and to add or delete interfaces or VLANs to or from an existing SPAN or RSPAN session, use the **monitor session destination** global configuration command. To remove the SPAN or RSPAN session or to remove destination interfaces from the SPAN or RSPAN session, use the **no** form of this command.

```
monitor session session-number destination {interface interface-id [, | -] [encapsulation
{replicate | dot1q} ] {ingress [dot1q | untagged] } | {remote} vlan vlan-id
no monitor session session-number destination {interface interface-id [, | -] [encapsulation
{replicate | dot1q} ] {ingress [dot1q | untagged] } | {remote} vlan vlan-id
```

Syntax Description	<i>session-number</i>
---------------------------	-----------------------

interface <i>interface-id</i>	Specifies the destination or source interface for a SPAN or RSPAN session. Valid interfaces are physical ports (including type, stack member, module, and port number). For source interface, port channel is also a valid interface type, and the valid range is 1 to 128.
,	(Optional) Specifies a series of interfaces or VLANs, or separates a range of interfaces or VLANs from a previous range. Enter a space before and after the comma.
-	(Optional) Specifies a range of interfaces or VLANs. Enter a space before and after the hyphen.
encapsulation replicate	(Optional) Specifies that the destination interface replicates the source interface encapsulation method. If not selected, the default is to send packets in native form (untagged). These keywords are valid only for local SPAN. For RSPAN, the RSPAN VLAN ID overwrites the original VLAN ID; therefore, packets are always sent untagged. The encapsulation options are ignored with the no form of the command.
encapsulation dot1q	(Optional) Specifies that the destination interface accepts the source interface incoming packets with IEEE 802.1Q encapsulation. These keywords are valid only for local SPAN. For RSPAN, the RSPAN VLAN ID overwrites the original VLAN ID; therefore, packets are always sent untagged. The encapsulation options are ignored with the no form of the command.
ingress	Enables ingress traffic forwarding.
dot1q	(Optional) Accepts incoming packets with IEEE 802.1Q encapsulation with the specified VLAN as the default VLAN.
untagged	(Optional) Accepts incoming packets with untagged encapsulation with the specified VLAN as the default VLAN.
isl	Specifies ingress forwarding using ISL encapsulation.

monitor session destination

remote	Specifies the remote VLAN for an RSPAN source or destination session. The range is 2 to 1001 and 1006 to 4094.
	The RSPAN VLAN cannot be VLAN 1 (the default VLAN) or VLAN IDs 1002 to 1005 (reserved for Token Ring and FDDI VLANs).
vlan <i>vlan-id</i>	Sets the default VLAN for ingress traffic when used with only the ingress keyword.

Command Default	No monitor sessions are configured.				
	If encapsulation replicate is not specified on a local SPAN destination port, packets are sent in native form with no encapsulation tag.				
	Ingress forwarding is disabled on destination ports.				
	You can specify all , local , range <i>session-range</i> , or remote with the no monitor session command to clear all SPAN and RSPAN, all local SPAN, a range, or all RSPAN sessions.				
Command Modes	Global configuration				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				
Usage Guidelines	<p>A SPAN or RSPAN destination must be a physical port.</p> <p>You can have a maximum of 64 destination ports on a switch or a switch stack.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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 (-).</p> <p>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.</p> <p>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.</p> <p>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.</p>				

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
```

monitor session filter

This example shows how to configure the destination port for ingress traffic on VLAN 5 by using a security device that supports IEEE 802.1Q encapsulation. Egress traffic replicates the source; ingress traffic uses IEEE 802.1Q encapsulation.

```
Device(config)# monitor session 2 destination interface gigabitethernet1/0/2 encapsulation
dot1q ingress dot1q vlan 5
```

This example shows how to configure the destination port for ingress traffic on VLAN 5 by using a security device that does not support encapsulation. Egress traffic and ingress traffic are untagged.

```
Device(config)# monitor session 2 destination interface gigabitethernet1/0/2 ingress untagged
vlan 5
```

monitor session filter

To start a new flow-based SPAN (FSPAN) session or flow-based RSPAN (FRSPAN) source or destination session, or to limit (filter) SPAN source traffic to specific VLANs, use the **monitor session filter** global configuration command. To remove filters from the SPAN or RSPAN session, use the **no** form of this command.

```
monitor session session-number filter {vlan vlan-id [, | -] }
no monitor session session-number filter {vlan vlan-id [, | -] }
```

Syntax Description	<i>session-number</i>	
	vlan <i>vlan-id</i>	Specifies a list of VLANs as filters on trunk source ports to limit SPAN source traffic to specific VLANs. The <i>vlan-id</i> range is 1 to 4094.
	,	(Optional) Specifies a series of VLANs, or separates a range of VLANs from a previous range. Enter a space before and after the comma.
	-	(Optional) Specifies a range of VLANs. Enter a space before and after the hyphen.
Command Default	No monitor sessions are configured.	
Command Modes	Global configuration	
Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.
Usage Guidelines	<p>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.</p> <p>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 (-).</p>	

VLAN filtering refers to analyzing network traffic on a selected set of VLANs on trunk source ports. By default, all VLANs are monitored on trunk source ports. You can use the **monitor session session_number filter vlan vlan-id** command to limit SPAN traffic on trunk source ports to only the specified VLANs.

VLAN monitoring and VLAN filtering are mutually exclusive. If a VLAN is a source, VLAN filtering cannot be enabled. If VLAN filtering is configured, a VLAN cannot become a source.

You can verify your settings by entering the **show monitor** privileged EXEC command. You can display SPAN, RSPAN, FSPAN, and FRSPAN configuration on the switch by entering the **show running-config** privileged EXEC command. SPAN information appears near the end of the output.

Examples

This example shows how to limit SPAN traffic in an existing session only to specific VLANs:

```
Switch(config)# monitor session 1 filter vlan 100 - 110
```

This example shows how to create a local SPAN session 1 to monitor both sent and received traffic on source port 1 on stack member 1 to destination port 2 on stack member 2 and to filter IPv4 traffic using access list number 122 in an FSPAN session:

```
Switch(config)# monitor session 1 source interface gigabitethernet1/0/1 both
Switch(config)# monitor session 1 destination interface gigabitethernet1/0/2
Switch(config)# monitor session 1 filter ip access-group 122
```

monitor session source

To start a new Switched Port Analyzer (SPAN) session or Remote SPAN (RSPAN) source session, or to add or delete interfaces or VLANs to or from an existing SPAN or RSPAN session, use the **monitor session source** global configuration command. To remove the SPAN or RSPAN session or to remove source interfaces from the SPAN or RSPAN session, use the **no** form of this command.

```
monitor session session_number source {interface interface-id [, | -] [both | rx | tx] |
[remote] vlan vlan-id [, | -] [both | rx | tx]}
no monitor session session_number source {interface interface-id [, | -] [both | rx | tx] |
[remote] vlan vlan-id [, | -] [both | rx | tx]}
```

Syntax Description

session_number

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.

monitor session source

-	(Optional) Specifies a range of interfaces or VLANs. Enter a space before and after the hyphen.
both rx tx	(Optional) Specifies the traffic direction to monitor. If you do not specify a traffic direction, the source interface sends both transmitted and received traffic.
remote	(Optional) Specifies the remote VLAN for an RSPAN source or destination session. The range is 2 to 1001 and 1006 to 4094. The RSPAN VLAN cannot be VLAN 1 (the default VLAN) or VLAN IDs 1002 to 1005 (reserved for Token Ring and FDDI VLANs).
vlan <i>vlan-id</i>	When used with only the ingress keyword, sets default VLAN for ingress traffic.

Command Default

- No monitor sessions are configured.
- On a source interface, the default is to monitor both received and transmitted traffic.
- On a trunk interface used as a source port, all VLANs are monitored.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Everest 16.6.1	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
```

monitor session type erspan-source

To configure a local Encapsulated Remote Switched Port Analyzer (ERSPAN) source session, use the **monitor session type erspan-source** command in global configuration mode. To remove the ERSPAN configuration, use the **no** form of this command.

```
monitor session span-session-number type erspan-source
no monitor session span-session-number type erspan-source
```

Syntax Description	<i>span-session-number</i>	Number of the local ERSPAN session. Valid values are from 1 to 66.
---------------------------	----------------------------	--

Command Default	ERSPAN source session is not configured.
------------------------	--

Command Modes	Global configuration (config)
----------------------	-------------------------------

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

Usage Guidelines	The <i>span-session-number</i> and the session type (configured by the <i>erspan-source</i> keyword) cannot be changed once configured. Use the no form of this command to remove the session and then re-create the session with a new session ID or a new session type.
-------------------------	--

The ERSPAN source session destination IP address, which must be configured on an interface on the destination switch, is the source of traffic that an ERSPAN destination session sends to the destination ports. You can

configure the same address in both the source and destination sessions with the **ip address** command in ERSPAN monitor destination session configuration mode.

The ERSPAN ID differentiates the ERSPAN traffic arriving at the same destination IP address from different ERSPAN source sessions.

The maximum local ERSPAN source session limit is 8.

Examples

The following example shows how to configure an ERSPAN source session number:

```
Switch(config)# monitor session 55 type erspan-source
Switch(config-mon-erspan-src) #
```

Related Commands

Command	Description
monitor session type	Creates an ERSPAN source session number or enters the ERSPAN session configuration mode for the session.
show capability feature monitor	Displays information about monitor features.
show monitor session	Displays information about the ERSPAN, SPAN, and RSPAN sessions.

origin

To configure the IP address used as the source of the Encapsulated Remote Switched Port Analyzer (ERSPAN) traffic, use the **origin** command in ERSPAN monitor destination session configuration mode. To remove the configuration, use the **no** form of this command.

```
origin ip-address
no origin ip-address
```

Syntax Description

ip-address Specifies the ERSPAN source session destination IP address.

Command Default

Source IP address is not configured.

Command Modes

ERSPAN monitor destination session configuration mode (config-mon-erspan-src-dst)

Command History

Release	Modification
---------	--------------

Cisco IOS XE Denali 16.3.1 This command was introduced.

Usage Guidelines

ERSPAN source session on a switch can use different source IP addresses using the **origin** command.

Examples

The following example shows how to configure an IP address for an ERSPAN source session:

```
Switch(config)# monitor session 2 type erspan-source
Switch(config-mon-erspan-src) # destination
```

```
Switch(config-mon-erspan-src-dst) # origin ip-address 203.0.113.2
```

The following sample output from the **show monitor session all** command displays ERSPAN source sessions with different source IP addresses:

```
Session 3
-----
Type : ERSPAN Source Session
Status : Admin Enabled
Source Ports :
Both : Gi1/0/13
Destination IP Address : 10.10.10.10
Origin IP Address : 10.10.10.10

Session 4
-----
Type : ERSPAN Source Session
Status : Admin Enabled
Destination IP Address : 192.0.2.1
Origin IP Address : 203.0.113.2
```

Related Commands

Command	Description
destination	Configures an ERSPAN destination session and specifies destination properties.
monitor session type erspan-source	Configures a local ERSPAN source session.

show ip sla statistics

To display current or aggregated operational status and statistics of all Cisco IOS IP Service Level Agreement (SLA) operations or a specified operation, use the **show ip sla statistics** command in user EXEC or privileged EXEC mode.

```
show ip sla statistics [operation-number [details] | aggregated [operation-number | details] | details]
```

Syntax Description

<i>operation-number</i>	(Optional) Number of the operation for which operational status and statistics are displayed. Accepted values are from 1 to 2147483647.
details	(Optional) Specifies detailed output.
aggregated	(Optional) Specifies the IP SLA aggregated statistics.

Command Default

Displays output for all running IP SLA operations.

Command Modes

User EXEC

Privileged EXEC

show capability feature monitor

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines	Use the show ip sla statistics to display the current state of IP SLA operations, including how much life the operation has left, whether the operation is active, and the completion time. The output also includes the monitoring data returned for the last (most recently completed) operation. This generated operation ID is displayed when you use the show ip sla configuration command for the base multicast operation, and as part of the summary statistics for the entire operation.
	Enter the show command for a specific operation ID to display details for that one responder.

Examples

The following is sample output from the **show ip sla statistics** command:

```
Device# show ip sla statistics

Current Operational State
Entry Number: 3
Modification Time: *22:15:43.000 UTC Sun Feb 11 2001
Diagnostics Text:
Last Time this Entry was Reset: Never
Number of Octets in use by this Entry: 1332
Number of Operations Attempted: 2
Current Seconds Left in Life: 3511
Operational State of Entry: active
Latest Completion Time (milliseconds): 544
Latest Operation Start Time: *22:16:43.000 UTC Sun Feb 11 2001
Latest Oper Sense: ok
Latest Sense Description: 200 OK
Total RTT: 544
DNS RTT: 12
TCP Connection RTT: 28
HTTP Transaction RTT: 504
HTTP Message Size: 9707
```

show capability feature monitor

To display information about monitor features, use the **show capability feature monitor** command in privileged EXEC mode.

show capability feature monitor {erspan-destination | erspan-source}

Syntax Description	erspan-destination	Displays information about the configured Encapsulated Remote Switched Port Analyzer (ERSPAN) source sessions.
	erspan-source	Displays all the configured global built-in templates.

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

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

Examples The following is sample output from the **show capability feature monitor erspan-source** command:

```
Switch# show capability feature monitor erspan-source

ERSPAN Source Session Supported: true
No of Rx ERSPAN source session: 8
No of Tx ERSPAN source session: 8
ERSPAN Header Type supported: II
ACL filter Supported: true
Fragmentation Supported: true
Truncation Supported: false
Sequence number Supported: false
QOS Supported: true
```

The following is sample output from the **show capability feature monitor erspan-destination** command:

```
Switch# show capability feature monitor erspan-destination

ERSPAN Destination Session Supported: false
```

Related Commands	Command	Description
	monitor session type erspan-source	Creates an ERSPAN source session number or enters the ERSPAN session configuration mode for the session.

show monitor

To display information about all Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) sessions, use the **show monitor** command in EXEC mode.

```
show monitor [session {session_number | all | local | range list | remote} [detail]]
```

Syntax Description	session	(Optional) Displays information about specified SPAN sessions.
	<i>session_number</i>	
	all	(Optional) Displays all SPAN sessions.
	local	(Optional) Displays only local SPAN sessions.

show monitor

range <i>list</i>	(Optional) Displays a range of SPAN sessions, where <i>list</i> is the range of valid sessions. The range is either a single session or a range of sessions described by two numbers, the lower one first, separated by a hyphen. Do not enter any spaces between comma-separated parameters or in hyphen-specified ranges.
	Note This keyword is available only in privileged EXEC mode.
remote	(Optional) Displays only remote SPAN sessions.
detail	(Optional) Displays detailed information about the specified sessions.

Command Modes User EXEC

Privileged EXEC

Command History **Release** **Modification**

Cisco IOS XE Everest 16.6.1 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 : Gi4/0/12
Encapsulation : Replicate
Ingress : Enabled, default VLAN = 4
Ingress encap : Untagged
```

show monitor capture

To display monitor capture (Wireshark) content, use the **show monitor capture file** command in privileged EXEC mode.

show monitor capture [capture-name [buffer] | file file-location : file-name] [brief | detailed | display-filter display-filter-string]

Syntax Description

<i>capture-name</i>	(Optional) Specifies the name of the capture to be displayed.
buffer	(Optional) Specifies that a buffer associated with the named capture is to be displayed.
file <i>file-location : file-name</i>	(Optional) Specifies the file location and name of the capture storage file to be displayed.
brief	(Optional) Specifies the display content in brief.
detailed	(Optional) Specifies detailed display content.
display-filter <i>display-filter-string</i>	Filters the display content according to the <i>display-filter-string</i> .

show monitor session

Command Default	Displays all capture content.	
Command Modes	Privileged EXEC	
Command History	Release	Modification
	This command was introduced.	

Usage Guidelines none

Example

To display the capture for a capture called mycap:

```
Device# show monitor capture mycap

Status Information for Capture mycap
  Target Type:
  Interface: CAPWAP,
    Ingress:
    0
    Egress:
    0
    Status : Active
    Filter Details:
      Capture all packets
    Buffer Details:
      Buffer Type: LINEAR (default)
    File Details:
      Associated file name: flash:mycap.pcap
      Size of buffer(in MB): 1
    Limit Details:
      Number of Packets to capture: 0 (no limit)
      Packet Capture duration: 0 (no limit)
      Packet Size to capture: 0 (no limit)
      Packets per second: 0 (no limit)
      Packet sampling rate: 0 (no sampling)
```

show monitor session

To display information about all Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) sessions, use the **show monitor session** command in EXEC mode.

```
show monitor session {session_number | all | erspan-source | local | range list | remote}
[detail]
```

Syntax Description	<i>session_number</i>	The session number identified with the SPAN or RSPAN session. The range is 1 to 68. However if this switch is stacked with Catalyst 2960-S switches, you are limited to a combined maximum of two local SPAN sessions and RSPAN source sessions, and the range is 1 to 66.
---------------------------	-----------------------	--

all	Displays all SPAN sessions.
erspan-source	Displays only source ERSPAN sessions.
local	Displays only local SPAN sessions.
range <i>list</i>	Displays a range of SPAN sessions, where <i>list</i> is the range of valid sessions. The range is either a single session or a range of sessions described by two numbers, the lower one first, separated by a hyphen. Do not enter any spaces between comma-separated parameters or in hyphen-specified ranges.
	Note This keyword is available only in privileged EXEC mode.
remote	Displays only remote SPAN sessions.
detail	(Optional) Displays detailed information about the specified sessions.

Command Modes	User EXEC (>) Privileged EXEC (#)
Command History	Release Cisco IOS XE Everest 16.6.1 Modification This command was introduced.
Usage Guidelines	The maximum local ERSPAN source session limit is 8.

Examples

The following is sample output from the **show monitor session** command for local SPAN source session 1:

```
Device# show monitor session 1
Session 1
-----
Type : Local Session
Source Ports :
RX Only : Gi4/0/1
Both : Gi4/0/2-3,Gi4/0/5-6
Destination Ports : Gi4/0/20
Encapsulation : Replicate
Ingress : Disabled
```

The following is sample output from the **show monitor session all** command when ingress traffic forwarding is enabled:

```
Device# show monitor session all
Session 1
-----
```

show platform software fed switch ip wccp

```
Type : Local Session
Source Ports :
Both : Gi4/0/2
Destination Ports : Gi4/0/3
Encapsulation : Native
Ingress : Enabled, default VLAN = 5
Ingress encap : DOT1Q
Session 2
-----
Type : Local Session
Source Ports :
Both : Gi4/0/8
Destination Ports : Gi4/0/12
Encapsulation : Replicate
Ingress : Enabled, default VLAN = 4
Ingress encap : Untagged
```

The following is sample output from the **show monitor session erspan-source** command:

```
Switch# show monitor session erspan-source

Type : ERSPAN Source Session
Status : Admin Enabled
Source Ports :
RX Only : Gi1/4/33
Destination IP Address : 20.20.163.20
Destination ERSPAN ID : 110
Origin IP Address : 10.10.10.216
IPv6 Flow Label : None
```

show platform software fed switch ip wccp

To display platform-dependent Web Cache Communication Protocol (WCCP) information, use the **show platform software fed switch ip wccp** privileged EXEC command.

```
show platform software fed switch{switch-number|active|standby}ip
wccp{cache-engines | interfaces | service-groups}
```

Syntax Description

switch{switch_num|active|standby} The device for which you want to display information.

- **switch_num**—Enter the switch ID. Displays information for the specified switch.
- **active**—Displays information for the active switch.
- **standby**—Displays information for the standby switch, if available.

cache-engines	Displays WCCP cache engines.
interfaces	Displays WCCP interfaces.
service-groups	Displays WCCP service groups.

Command Modes	Privileged EXEC			
Command History	Release	Modification		
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:				
<pre>Device# show platform software fed switch 1 ip wccp interfaces WCCP Interface Info ===== **** WCCP Interface: Port-channel13 iif_id: 000000000000007c (#SG:3), VRF: 0 Ingress WCCP ***** port_handle:0x20000f9 List of Service Groups on this interface: * Service group id:90 vrf_id:0 (ref count:24) type: Dynamic Open service prot: PROT_TCP 14_type: Dest ports priority: 35 Promiscuous mode (no ports). * Service group id:70 vrf_id:0 (ref count:24) type: Dynamic Open service prot: PROT_TCP 14_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 14_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 14_type: Dest ports priority: 35 Promiscuous mode (no ports). * Service group id:70 vrf_id:0 (ref count:24) type: Dynamic Open service prot: PROT_TCP 14_type: Dest ports priority: 35 Promiscuous mode (no ports). <output truncated></pre>				

show platform software swspan

show platform software swspan

To display switched port analyzer (SPAN) information, use the **show platform software swspan** command in privileged EXEC mode.

```
show platform software swspan {switch} {{F0 | FP active} counters} | R0 | RP active} {destination sess-id session-ID | source sess-id session-ID}
```

Syntax Description	
switch	Displays information about the switch.
F0	Displays information about the Embedded Service Processor (ESP) slot 0.
FP	Displays information about the ESP.
active	Displays information about the active instance of the ESP or the Route Processor (RP).
counters	Displays the SWSPAN message counters.
R0	Displays information about the RP slot 0.
RP	Displays information the RP.
destination sess-id session-ID	Displays information about the specified destination session.
source sess-id session-ID	Displays information about the specified source session.

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

Command History	Release	Modification
	Cisco IOS XE Denali 16.1.1	This command was introduced in a release prior to Cisco IOS XE Denali 16.1.1.

Usage Guidelines	If the session number does not exist or if the SPAN session is a remote destination session, the command output will display the following message "% Error: No Information Available."
-------------------------	---

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 swwspn RP active destination** command:

```

Switch# show platform software swwspn 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.

snmp-server enable traps**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 | wlancreate | 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 | wlancreate | 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

snmp-server enable traps bridge

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.
Usage Guidelines	<p>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.</p> <p>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.</p> <p>When supported, use the snmp-server enable traps command to enable sending of traps or informs.</p>	
	 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.	
Examples	<p>This example shows how to enable more than one type of SNMP trap:</p> <pre>Device(config)# snmp-server enable traps config Device(config)# snmp-server enable traps vtp</pre>	
<h2>snmp-server enable traps bridge</h2>		
Command Default	<p>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.</p>	
Syntax Description	<p>snmp-server enable traps bridge [newroot] [topologychange] no snmp-server enable traps bridge [newroot] [topologychange]</p>	
	<p>newroot (Optional) Enables SNMP STP bridge MIB new root traps.</p>	
	<p>topologychange (Optional) Enables SNMP STP bridge MIB topology change traps.</p>	
Command Default	<p>The sending of bridge SNMP traps is disabled.</p>	
Command Modes	<p>Global configuration</p>	

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	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 Everest 16.6.1	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.	

snmp-server enable traps call-home

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 Everest 16.6.1	This command was introduced.

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 Everest 16.6.1	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 envmon

```
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 Everest 16.6.1	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.



Note

Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples

This example shows how to generate CPU threshold notifications:

```
Device(config)# snmp-server enable traps cpu threshold
```

snmp-server enable traps envmon

To enable SNMP environmental traps, use the **snmp-server enable traps envmon** command in global configuration mode. Use the **no** form of this command to return to the default setting.

```
snmp-server enable traps envmon [fan] [shutdown] [status] [supply] [temperature]
no snmp-server enable traps envmon [fan] [shutdown] [status] [supply] [temperature]
```

Syntax Description

fan (Optional) Enables fan traps.

shutdown (Optional) Enables environmental monitor shutdown traps.

status (Optional) Enables SNMP environmental status-change traps.

supply (Optional) Enables environmental monitor power-supply traps.

temperature (Optional) Enables environmental monitor temperature traps.

Command Default

The sending of environmental SNMP traps is disabled.

Command Modes	Global configuration			
Command History	Release	Modification		
	Cisco IOS XE Everest 16.6.1	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.			
	<p>Note Informs are not supported in SNMPv1.</p> <p>To enable more than one type of trap, you must enter a separate snmp-server enable traps command for each trap type.</p>			
Examples	This example shows how to generate fan traps:			
	<pre>Device(config)# snmp-server enable traps envmon fan</pre>			
<h2>snmp-server enable traps errdisable</h2>				
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.				
<pre>snmp-server enable traps errdisable [notification-rate number-of-notifications] no snmp-server enable traps errdisable [notification-rate number-of-notifications]</pre>				
Syntax Description	<p>notification-rate <i>number-of-notifications</i> (Optional) Specifies number of notifications per minute as the notification rate. Accepted values are from 0 to 10000.</p>			
Command Default	The sending of SNMP notifications of error-disabling is disabled.			
Command Modes	Global configuration			
Command History	Release	Modification		
	Cisco IOS XE Everest 16.6.1	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.			
	<p>Note Informs are not supported in SNMPv1.</p>			

snmp-server enable traps flash

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 Everest 16.6.1	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	<table border="1"> <thead> <tr> <th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td><td>This command was introduced.</td></tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	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.
---------------------------	--

snmp-server enable traps mac-notification

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 Everest 16.6.1	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 Everest 16.6.1	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:	
	<pre>Device(config)# snmp-server enable traps mac-notification change</pre>	
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.	
	<pre>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]</pre>	
Syntax Description	<p>cisco-specific (Optional) Enables Cisco-specific traps.</p> <p>errors (Optional) Enables error traps.</p> <p>lsa (Optional) Enables link-state advertisement (LSA) traps.</p> <p>rate-limit (Optional) Enables rate-limit traps.</p> <p>rate-limit-time (Optional) Specifies window of time in seconds for rate-limit traps. Accepted values are 2 to 60.</p> <p>max-number-of-traps (Optional) Specifies maximum number of rate-limit traps to be sent in window time.</p> <p>retransmit (Optional) Enables packet-retransmit traps.</p> <p>state-change (Optional) Enables state-change traps.</p>	
Command Default	The sending of OSPF SNMP traps is disabled.	
Command Modes	Global configuration	

snmp-server enable traps pim

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	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.	

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 Everest 16.6.1	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 (Optional) Sets the maximum number of port-security traps sent per second. The range is *value* 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 Everest 16.6.1		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
```

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 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	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				

Usage Guidelines Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.



Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples

This example shows how to enable power-over-Ethernet traps for group 1:

```
Device(config)# snmp-server enable traps power-over-ethernet group 1
```

snmp-server enable traps snmp

To enable SNMP traps, use the **snmp-server enable traps snmp** command in global configuration mode. Use the **no** form of this command to return to the default setting.

```
snmp-server enable traps snmp [authentication] [coldstart] [linkdown] [linkup] [warmstart]
no snmp-server enable traps snmp [authentication] [coldstart] [linkdown] [linkup]
] [warmstart]
```

Syntax Description	authentication (Optional) Enables authentication traps.
---------------------------	--

coldstart	(Optional) Enables cold start traps.
linkdown	(Optional) Enables linkdown traps.
linkup	(Optional) Enables linkup traps.
warmstart	(Optional) Enables warmstart traps.

Command Default The sending of SNMP traps is disabled.

Command Modes Global configuration

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	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 <i>number-of-minutes</i>	(Optional) Specifies the SNMP storm-control trap rate in minutes. Accepted values are from 0 to 1000.
---------------------------	--	---

Command Default The sending of SNMP storm-control trap parameters is disabled.

Command Modes Global configuration

snmp-server enable traps stpx

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	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.	

Examples	This example shows how to set the SNMP storm-control trap rate to 10 traps per minute:
	<pre>Device(config)# snmp-server enable traps storm-control trap-rate 10</pre>

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 Everest 16.6.1	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

a (Optional) Enables all SNMP transceiver traps.

Command Default

The sending of SNMP transceiver traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Everest 16.6.1	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 vstack

```
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 Everest 16.6.1	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 Everest 16.6.1	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 <i>ip-address</i> 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 Everest 16.6.1	This command was introduced.
Usage Guidelines	None	

Examples

The following example configures a local engine ID of 1234000000000000000000000000:

```
Device(config)# snmp-server engineID local 1234
```

snmp-server host

To specify the recipient (host) of a Simple Network Management Protocol (SNMP) notification operation, use the **snmp-server host** global configuration command on the device. Use the **no** form of this command to remove the specified host.

```
snmp-server host {host-addr} [vrf vrf-instance] [informs | traps] [version {1 | 2c | 3
{auth | noauth | priv}}] {community-string [notification-type]}
no snmp-server host {host-addr} [vrf vrf-instance] [informs | traps] [version {1 | 2c |
3 {auth | noauth | priv}}] {community-string [notification-type]}
```

Syntax Description	<p>host-addr Name or Internet address of the host (the targeted recipient).</p> <p>vrf vrf-instance (Optional) Specifies the virtual private network (VPN) routing instance and name for this host.</p> <p>informs traps (Optional) Sends SNMP traps or informs to this host.</p> <p>version 1 2c 3 (Optional) Specifies the version of the SNMP used to send the traps.</p> <ul style="list-style-type: none"> 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. <p>auth noauth auth (Optional)—Enables Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication.</p> <p>noauth (Default)—The noAuthNoPriv security level. This is the default if the auth noauth priv keyword choice is not specified.</p> <p>priv (Optional)—Enables Data Encryption Standard (DES) packet encryption (also called privacy).</p>
--------------------	---

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.
- **ftp**—Sends SNMP VLAN Trunking Protocol (VTP) traps.

Command Default

This command is disabled by default. No notifications are sent.

If you enter this command with no keywords, the default is to send all trap types to the host. No informs are sent to this host.

If no **version** keyword is present, the default is Version 1.

If Version 3 is selected and no authentication keyword is entered, the default is the **noauth** (noAuthNoPriv) security level.



Note Though visible in the command-line help strings, the **fru-ctrl** keyword is not supported.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send acknowledgments when it receives traps. The sender cannot determine if the traps were received. However, an SNMP entity that receives an inform request acknowledges the message with an SNMP response.

PDU. If the sender never receives the response, the inform request can be sent again, so that informs are more likely to reach their intended destinations.

However, informs consume more resources in the agent and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Traps are also sent only once, but an inform might be retried several times. The retries increase traffic and contribute to a higher overhead on the network.

If you do not enter an **snmp-server host** command, no notifications are sent. To configure the device to send SNMP notifications, you must enter at least one **snmp-server host** command. If you enter the command with no keywords, all trap types are enabled for the host. To enable multiple hosts, you must enter a separate **snmp-server host** command for each host. You can specify multiple notification types in the command for each host.

If a local user is not associated with a remote host, the device does not send informs for the **auth** (authNoPriv) and the **priv** (authPriv) authentication levels.

When multiple **snmp-server host** commands are given for the same host and kind of notification (trap or inform), each succeeding command overwrites the previous command. Only the last **snmp-server host** command is in effect. For example, if you enter an **snmp-server host inform** command for a host and then enter another **snmp-server host inform** command for the same host, the second command replaces the first.

The **snmp-server host** command is used with the **snmp-server enable traps** global configuration command. Use the **snmp-server enable traps** command to specify which SNMP notifications are sent globally. For a host to receive most notifications, at least one **snmp-server enable traps** command and the **snmp-server host** command for that host must be enabled. Some notification types cannot be controlled with the **snmp-server enable traps** command. For example, some notification types are always enabled. Other notification types are enabled by a different command.

The **no snmp-server host** command with no keywords disables traps, but not informs, to the host. To disable informs, use the **no snmp-server host informs** command.

Examples

This example shows how to configure a unique SNMP community string named comaccess for traps and prevent SNMP polling access with this string through access-list 10:

```
Device(config)# snmp-server community comaccess ro 10
Device(config)# snmp-server host 172.20.2.160 comaccess
Device(config)# access-list 10 deny any
```

This example shows how to send the SNMP traps to the host specified by the name myhost.cisco.com. The community string is defined as comaccess:

```
Device(config)# snmp-server enable traps
Device(config)# snmp-server host myhost.cisco.com comaccess snmp
```

This example shows how to enable the device to send all traps to the host myhost.cisco.com by using the community string public:

```
Device(config)# snmp-server enable traps
Device(config)# snmp-server host myhost.cisco.com public
```

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

source (ERSPAN)

To configure the Encapsulated Remote Switched Port Analyzer (ERSPAN) source interface or VLAN, and the traffic direction to be monitored, use the **source** command in ERSPAN monitor source session configuration mode. To disable the configuration, use the **no** form of this command.

```
source {interface type number | vlan vlan-ID}{, | - | both | rx | tx}
```

Syntax Description

interface type number	Specifies an interface type and number.
vlan vlan-ID	Associates the ERSPAN source session number with VLANs. Valid values are from 1 to 4094.
,	(Optional) Specifies another interface.
-	(Optional) Specifies a range of interfaces.
both	(Optional) Monitors both received and transmitted ERSPAN traffic.
rx	(Optional) Monitors only received traffic.
tx	(Optional) Monitors only transmitted traffic.

Command Default

Source interface or VLAN is not configured.

Command Modes

ERSPAN monitor source session configuration mode (config-mon-erspan-src)

Command History

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines

You cannot include source VLANs and filter VLANs in the same session.

Examples

The following example shows how to configure ERSPAN source session properties:

```
Device(config)# monitor session 2 type erspan-source
Device(config-mon-erspan-src)# source interface fastethernet 0/1 rx
```

Related Commands

Command	Description
monitor session type	Configures a local ERSPAN source or destination session.

switchport mode access

To sets the interface as a nontrunking nontagged single-VLAN Ethernet interface , use the **switchport mode access** command in template configuration mode. Use the **no** form of this command to return to the default setting.

switchport mode access
no switchport mode access

Syntax Description	switchport mode access Sets the interface as a nontrunking nontagged single-VLAN Ethernet interface.	
Command Default	An access port can carry traffic in one VLAN only. By default, an access port carries traffic for VLAN1.	
Command Modes	Template configuration	
Command History	Release	Modification
		This command was introduced.
Examples	This example shows how to set a single-VLAN interface	

```
Device(config-template)# switchport mode access
```

switchport voice vlan

To specify to forward all voice traffic through the specified VLAN, use the **switchport voice vlan** command in template configuration mode. Use the **no** form of this command to return to the default setting.

switchport voice vlan*vlan_id*
no switchport voice vlan

Syntax Description	switchport voice vlan <i>vlan_id</i> Specifies to forward all voice traffic through the specified VLAN.	
Command Default	You can specify a value from 1 to 4094.	
Command Modes	Template configuration	
Command History	Release	Modification
	Cisco IOS XE Fuji 16.9.1	This command was introduced.
Examples	This example shows how to specify to forward all voice traffic through the specified VLAN.	

switchport voice vlan

```
Device(config-template)# switchport voice vlan 20
```

Flexible NetFlow Commands

- [cache](#), on page 632
- [clear flow exporter](#), on page 634
- [clear flow monitor](#), on page 635
- [collect](#), on page 636
- [collect counter](#), on page 637
- [collect interface](#), on page 637
- [collect timestamp absolute](#), on page 638
- [collect transport tcp flags](#), on page 639
- [datalink flow monitor](#), on page 640
- [debug flow exporter](#), on page 641
- [debug flow monitor](#), on page 641
- [debug flow record](#), on page 642
- [debug sampler](#), on page 643
- [description](#), on page 643
- [destination](#), on page 644
- [dscp](#), on page 645
- [export-protocol netflow-v9](#), on page 645
- [export-protocol netflow-v5](#), on page 646
- [exporter](#), on page 646
- [flow exporter](#), on page 647
- [flow monitor](#), on page 647
- [flow record](#), on page 648
- [ip flow monitor](#), on page 649
- [ipv6 flow monitor](#), on page 650
- [match datalink ethertype](#), on page 651
- [match datalink mac](#), on page 652
- [match datalink vlan](#), on page 653
- [match flow cts](#), on page 654
- [match flow direction](#), on page 654
- [match interface](#), on page 655
- [match ipv4](#), on page 656
- [match ipv4 destination address](#), on page 657
- [match ipv4 source address](#), on page 657

- [match ipv4 ttl, on page 658](#)
- [match ipv6, on page 658](#)
- [match ipv6 destination address, on page 659](#)
- [match ipv6 hop-limit, on page 660](#)
- [match ipv6 source address, on page 660](#)
- [match transport, on page 661](#)
- [match transport icmp ipv4, on page 662](#)
- [match transport icmp ipv6, on page 662](#)
- [mode random 1 out-of, on page 663](#)
- [option, on page 664](#)
- [record, on page 665](#)
- [sampler, on page 666](#)
- [show flow exporter, on page 666](#)
- [show flow interface, on page 668](#)
- [show flow monitor, on page 669](#)
- [show flow record, on page 671](#)
- [show sampler, on page 672](#)
- [source, on page 673](#)
- [template data timeout, on page 674](#)
- [transport, on page 675](#)
- [ttl, on page 676](#)

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:				
	<ul style="list-style-type: none"> • Cache type: normal • Active flow timeout: 1800 seconds 				
Command Modes	Flow monitor configuration				
Command History	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; padding-bottom: 2px;">Release</th><th style="text-align: left; padding-bottom: 2px;">Modification</th></tr> </thead> <tbody> <tr> <td style="padding-top: 2px;">Cisco IOS XE Everest 16.6.1</td><td>This command was introduced.</td></tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				
Usage Guidelines	<p>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.</p> <p>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.</p> <p>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.</p> <p>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).</p> <p>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.</p> <p>To return a cache to its default settings, use the default cache flow monitor configuration command.</p>				

**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
```

clear flow exporter

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 Everest 16.6.1 This command was introduced.

Usage Guidelines

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

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

Examples

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

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

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

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

clear flow monitor

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

```
clear flow monitor [name] monitor-name [{[cache] force-export | statistics}]
```

Syntax Description

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

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Everest 16.6.1	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:

collect

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

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

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

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

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

collect

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

collect {counter | interface | timestamp | transport}

Syntax Description	counter Configures the number of bytes or packets in a flow as a non-key field for a flow record. For more information, see collect counter, on page 637 .
	interface Configures the input and output interface name as a non-key field for a flow record. For more information, see collect interface, on page 637 .
	timestamp Configures the absolute time of the first seen or last seen packet in a flow as a non-key field for a flow record. For more information, see collect timestamp absolute, on page 638 .
	transport Enables the collecting of transport TCP flags from a flow record. For more information, see collect transport tcp flags, on page 639 .

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 Everest 16.6.1	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.

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 Everest 16.6.1	This command was introduced.

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

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

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

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

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

collect interface

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

```
collect interface input
no collect interface input
```

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

collect timestamp absolute

Command Default	The input interface name is not configured as a non-key field.	
Command Modes	Flow record configuration	
Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1 This command was introduced.	
Usage Guidelines	<p>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.</p> <p>To return this command to its default settings, use the no collect interface or default collect interface flow record configuration command.</p>	
	<p>The following example configures the input interface as a non-key field:</p> <pre>Device(config)# flow record FLOW-RECORD-1 Device(config-flow-record)# collect interface input</pre>	
<h2>collect timestamp absolute</h2>		
	<p>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.</p>	
	<pre>collect timestamp absolute {first last} no collect timestamp absolute {first last}</pre>	
Syntax Description	<p>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.</p> <p>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.</p>	
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 Everest 16.6.1 This command was introduced.	
Usage Guidelines	<p>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</p>	

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 Everest 16.6.1	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

datalink flow monitor

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

The following example collects the TCP flags from a flow:

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

datalink flow monitor

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

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

Syntax Description

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

Command Default

A flow monitor is not enabled.

Command Modes

Interface configuration

Command History

Release	Modification
----------------	---------------------

Cisco IOS XE Everest 16.6.1 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	<p>name (Optional) Specifies the name of a flow exporter.</p> <p><i>exporter-name</i> (Optional) The name of a flow exporter that was previously configured.</p> <p>error (Optional) Enables debugging for flow exporter errors.</p> <p>event (Optional) Enables debugging for flow exporter events.</p> <p>packets (Optional) Enables packet-level debugging for flow exporters.</p> <p>number (Optional) The number of packets to debug for packet-level debugging of flow exporters. The range is 1 to 65535.</p>				
Command Modes	Privileged EXEC				
Command History	<table border="1"> <thead> <tr> <th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td><td>This command was introduced.</td></tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	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	<p>error (Optional) Enables debugging for flow monitor errors for all flow monitors or for the specified flow monitor.</p> <p>name (Optional) Specifies the name of a flow monitor.</p> <p>monitor-name (Optional) Name of a flow monitor that was previously configured.</p> <p>cache (Optional) Enables debugging for the flow monitor cache.</p>
---------------------------	---

debug flow record

cache error	(Optional) Enables debugging for flow monitor cache errors.
packets	(Optional) Enables packet-level debugging for flow monitors.
<i>packets</i>	(Optional) Number of packets to debug for packet-level debugging of flow monitors. The range is 1 to 65535.

Command Modes	Privileged EXEC
----------------------	-----------------

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

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

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

debug flow record

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

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

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

Command Modes	Privileged EXEC
----------------------	-----------------

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Examples	The following example enables debugging for the flow record:
-----------------	--

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

debug sampler

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

```
debug sampler [{detailed | error | [name] sampler-name [{detailed | error | sampling samples}]}
no debug sampler [{detailed | error | [name] sampler-name [{detailed | error | sampling}]}
```

Syntax Description

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

Command Modes

Privileged EXEC

Command History

Release	Modification
---------	--------------

Cisco IOS XE Everest 16.6.1 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

<i>description</i>	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:

destination

Flow exporter configuration

Flow monitor configuration

Flow record configuration

Command History**Release** **Modification**

Cisco IOS XE Everest 16.6.1 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*}
no destination {*hostnameip-address*}

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.

Command Default

An export destination is not configured.

Command Modes

Flow exporter configuration

Command History**Release** **Modification**

Cisco IOS XE Everest 16.6.1 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 cache entry to a destination system:

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

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 Everest 16.6.1 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

export-protocol netflow-v5

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	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 Everest 16.6.1	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	<i>exporter-name</i> Name of a flow exporter that was previously configured.	
Command Default	An exporter is not configured.	
Command Modes	Flow monitor configuration	
Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	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 flow exporter, or to modify an existing flow exporter, and enter flow exporter configuration mode, use the **flow exporter** command in global configuration mode. To remove a 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

flow exporters are not present in the configuration.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Everest 16.6.1	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 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 record

```
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

flow monitors are not present in the configuration.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines

Flow monitors are the 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 flow record, or to modify an existing flow record, and enter flow record configuration mode, use the **flow record** command in global configuration mode. To remove a 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 flow record is not configured.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines

A flow record defines the keys that uses to identify packets in the flow, as well as other fields of interest that gathers for the flow. You can define a flow record with any combination of keys and fields of interest. The

supports a rich set of keys. A flow record also defines the types of counters gathered per flow. You can configure 64-bit packet or byte counters.

Examples

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

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

ip flow monitor

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

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

Syntax Description

<i>monitor-name</i>	Name of the flow monitor to apply to the interface.
---------------------	---

sampler <i>sampler-name</i>	(Optional) Enables the specified flow sampler for the flow monitor.
------------------------------------	---

input	Monitors IPv4 traffic that the device receives on the interface.
--------------	--

Command Default

A flow monitor is not enabled.

Command Modes

Interface configuration

Command History

Release	Modification
----------------	---------------------

Cisco IOS XE Everest 16.6.1	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
```

ipv6 flow monitor

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

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

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

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

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

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

ipv6 flow monitor

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

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

Syntax Description	<p><i>monitor-name</i> Name of the flow monitor to apply to the interface.</p> <p>sampler <i>sampler-name</i> (Optional) Enables the specified flow sampler for the flow monitor.</p> <p>input Monitors IPv6 traffic that the device receives on the interface.</p>				
Command Default	A flow monitor is not enabled.				
Command Modes	Interface configuration				
Command History	<table border="1"> <thead> <tr> <th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td><td>This command was introduced.</td></tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				
Usage Guidelines	<p>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.</p> <p>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.</p> <p>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.</p>				

**Note**

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

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

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

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

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

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

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

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

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

match datalink ethertype

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

match datalink ethertype
no match datalink ethertype

Syntax Description

This command has no arguments or keywords.

Command Default

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

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced.

match datalink mac**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 flow record:

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

match datalink mac

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

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

Syntax Description	destination address	Configures the use of the destination MAC address as a key field.
	input	Specifies the MAC address of input packets.
	source address	Configures the use of the source MAC address as a key field.
Command Default	MAC addresses are not configured as a key field.	
Command Modes	Flow record configuration	
Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1 This command was introduced.	
Usage Guidelines	A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the match command.	

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



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

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

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

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

match datalink vlan

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

```
match datalink vlan input
no match datalink vlan input
```

Syntax Description

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

Command Default

The VLAN ID is not configured as a key field.

Command Modes

Flow record configuration

Command History

Release	Modification
---------	--------------

Cisco IOS XE Everest 16.6.1 This command was introduced.

Usage Guidelines

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

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

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

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

match flow cts

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	<table border="1"> <thead> <tr> <th style="text-align: left;">Release</th><th style="text-align: left;">Modification</th></tr> </thead> <tbody> <tr> <td></td><td>This command was introduced.</td></tr> <tr> <td></td><td>This command was reintroduced. This command was not supported in</td></tr> </tbody> </table>	Release	Modification		This command was introduced.		This command was reintroduced. This command was not supported in
Release	Modification						
	This command was introduced.						
	This command was reintroduced. This command was not supported in						

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 Everest 16.6.1 This command was introduced.	
Usage Guidelines	<p>A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the match command.</p> <p>The 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.</p>	
	<p>The following example configures the direction the flow was monitored in as a key field:</p> <pre>Device(config)# flow record FLOW-RECORD-1 Device(config-flow-record)# match flow direction</pre>	
<h2>match interface</h2>		
	<p>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.</p>	
	<pre>match interface {input output} no match interface {input output}</pre>	
Syntax Description	<p>input Configures the input interface as a key field.</p> <p>output Configures the output interface as a key field.</p>	
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 Everest 16.6.1 This command was introduced.	
Usage Guidelines	<p>A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the match command.</p> <p>The following example configures the input interface as a key field:</p>	

match ipv4

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

Syntax Description	destination address Configures the IPv4 destination address as a key field. For more information see match ipv4 destination address, on page 657 .				
	protocol Configures the IPv4 protocol as a key field.				
	source address Configures the IPv4 destination address as a key field. For more information see match ipv4 source address, on page 657 .				
	tos Configures the IPv4 ToS as a key field.				
	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	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	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 Everest 16.6.1	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 Everest 16.6.1	This command was introduced.

match ipv4 ttl**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 Everest 16.6.1	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 | protocol | source address | traffic-class | version}
no match ipv6 {destination address | protocol | source address | traffic-class | version}
```

Syntax Description		
destination address	Configures the IPv4 destination address as a key field. For more information see match ipv6 destination address, on page 659 .	
protocol	Configures the IPv6 protocol as a key field.	
source address	Configures the IPv4 destination address as a key field. For more information see match ipv6 source address, on page 660 .	
Command Default	The IPv6 fields are not configured as a key field.	
Command Modes	Flow record configuration	
Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1 This command was introduced.	
Usage Guidelines	<p>A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the match command.</p> <p>The following example configures the IPv6 protocol field as a key field:</p> <pre>Device(config)# flow record FLOW-RECORD-1 Device(config-flow-record)# match ipv6 protocol</pre>	

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 Everest 16.6.1 This command was introduced.	
Usage Guidelines	<p>A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the match command.</p>	

match ipv6 hop-limit

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 Everest 16.6.1	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 Everest 16.6.1 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.

Syntax Description	destination-port Configures the transport destination port 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 Everest 16.6.1 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:	
	<pre>Device(config)# flow record FLOW-RECORD-1 Device(config-flow-record)# match transport destination-port</pre>	
	The following example configures the source port as a key field:	
	<pre>Device(config)# flow record FLOW-RECORD-1 Device(config-flow-record)# match transport source-port</pre>	

match transport icmp ipv4

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 Everest 16.6.1	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	<table border="1"> <thead> <tr> <th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td><td>This command was introduced.</td></tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	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:				
	<pre>Device(config)# flow record FLOW-RECORD-1 Device(config-flow-record)# match transport icmp ipv6 code</pre>				
	The following example configures the IPv6 ICMP type field as a key field:				
	<pre>Device(config)# flow record FLOW-RECORD-1 Device(config-flow-record)# match transport icmp ipv6 type</pre>				

mode random 1 out-of

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

```
mode random 1 out-of window-size
no mode
```

Syntax Description	<i>window-size</i> 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	<table border="1"> <thead> <tr> <th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td><td>This command was introduced.</td></tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				
Usage Guidelines	A total of four unique samplers are supported on the . Packets are chosen in a manner that should eliminate any bias from traffic patterns and counter any attempt by users to avoid monitoring.				
Note	The deterministic keyword is not supported, even though it is visible in the command-line help string.				

option**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 , 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 Everest 16.6.1	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 flow monitor, use the **record** command in flow monitor configuration mode. To remove a flow record for a 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 Everest 16.6.1	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

sampler

To create a flow sampler, or to modify an existing flow sampler, and to enter 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

flow samplers are not configured.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines

Flow samplers are used to reduce the load placed by 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 packets. Flow samplers are applied to interfaces in conjunction with a flow monitor to implement sampled .

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 [{export-ids netflow-v9|[name] exporter-name [{statistics | templates}] | statistics | templates}]
```

Syntax Description

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	<table border="1"> <thead> <tr> <th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td><td>This command was introduced.</td></tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	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.

show flow interface

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

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

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

show flow interface

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

show flow interface [type number]

Syntax Description	<p><i>type</i> (Optional) The type of interface on which you want to display accounting configuration information.</p> <p><i>number</i> (Optional) The number of the interface on which you want to display accounting configuration information.</p>				
Command Modes	Privileged EXEC				
Command History	<table> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				

Examples

The following example displays the 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:	<p>The direction of traffic that is being monitored by the flow monitor.</p> <p>The possible values are:</p> <ul style="list-style-type: none"> • Input—Traffic is being received by the interface. • Output—Traffic is being transmitted by the interface.
traffic(ip)	<p>Indicates if the flow monitor is in normal mode or sampler mode.</p> <p>The possible values are:</p> <ul style="list-style-type: none"> • 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 flow monitor, use the **show flow monitor** command in privileged EXEC mode.

Syntax Description	
name	(Optional) Specifies the name of a flow monitor.
<i>monitor-name</i>	(Optional) Name of a flow monitor that was previously configured.
cache	(Optional) Displays the contents of the cache for the flow monitor.
format	(Optional) Specifies the use of one of the format options for formatting the display output.
csv	(Optional) Displays the flow monitor cache contents in comma-separated variables (CSV) format.
record	(Optional) Displays the flow monitor cache contents in record format.
table	(Optional) Displays the flow monitor cache contents in table format.
statistics	(Optional) Displays the statistics for the flow monitor.

Command Modes	Privileged EXEC
----------------------	-----------------

show flow monitor

Command History

Release	Modification
Cisco IOS XE Everest 16.6.1	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 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 collects values as additional data for the cache.

Examples

The following example displays the status for a flow monitor:

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

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

This table describes the significant fields shown in the display.

Table 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 value is always normal, as it is the only supported cache type.
Status	Status of the flow monitor cache. The possible values are: <ul style="list-style-type: none"> • allocated—The cache is allocated. • being deleted—The cache is being deleted. • not allocated—The cache is not allocated.

Field	Description
Size	Current cache size.
Inactive Timeout	Current value for the inactive timeout in seconds.
Active Timeout	Current value for the active timeout in seconds.

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

This table describes the significant fields shown in the display.

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

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

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

show flow record

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

show flow record [{[name]} record-name]

Syntax Description	name (Optional) Specifies the name of a flow record.				
	<i>record-name</i> (Optional) Name of a user-defined flow record that was previously configured.				
Command Default	None				
Command Modes	Privileged EXEC				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	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

show sampler

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

show sampler [{name] sampler-name}]

Syntax Description	name (Optional) Specifies the name of a sampler. <i>sampler-name</i> (Optional) Name of a sampler that was previously configured.				
Command Default	None				
Command Modes	Privileged EXEC				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	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 106: show sampler Field Descriptions

Field	Description
ID	ID number of the flow sampler.
Export ID	ID of the flow sampler export.

Field	Description
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 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 flow exporter, use the **no** form of this command.

```
source interface-type interface-number
no source
```

Syntax Description	<code>interface-type</code> Type of interface whose IP address you want to use for the source IP address of the packets sent by a flow exporter. <code>interface-number</code> Interface number whose IP address you want to use for the source IP address of the packets sent by a flow exporter.				
Command Default	The IP address of the interface over which the datagram is transmitted is used as the source IP address.				
Command Modes	Flow exporter configuration				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				
Usage Guidelines	The benefits of using a consistent IP source address for the datagrams that sends include the following:				

template data timeout

- The source IP address of the datagrams exported by is used by the destination system to determine from which device the data is arriving. If your network has two or more paths that can be used to send 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 datagrams from the same device, but with different source IP addresses. When the destination system receives datagrams from the same device with different source IP addresses, the destination system treats the datagrams as if they were being sent from different devices. To avoid having the destination system treat the datagrams as if they were being sent from different devices, you must configure the destination system to aggregate the datagrams it receives from all of the possible source IP addresses in the device into a single 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 traffic. Creating and maintaining access lists for permitting traffic from known sources and blocking it from unknown sources is easier when you limit the source IP address for datagrams to a single IP address for each device that is exporting 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 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 to use a loopback interface as the source interface for NetFlow traffic:

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

template data timeout

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

```
template data timeout seconds
no template data timeout seconds
```

Syntax Description	<i>seconds</i> Timeout value in seconds. The range is 1 to 86400. The default is 600.				
Command Default	The default template resend timeout for a flow exporter is 600 seconds.				
Command Modes	Flow exporter configuration				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				
Usage Guidelines	<p>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.</p> <p>To return this command to its default settings, use the no template data timeout or default template data timeout flow record exporter command.</p>				

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

```
transport udp udp-port
no transport udp udp-port
```

Syntax Description	udp <i>udp-port</i> Specifies User Datagram Protocol (UDP) as the transport protocol and the UDP port number.				
Command Default	Flow exporters use UDP on port 9995.				
Command Modes	Flow exporter configuration				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	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

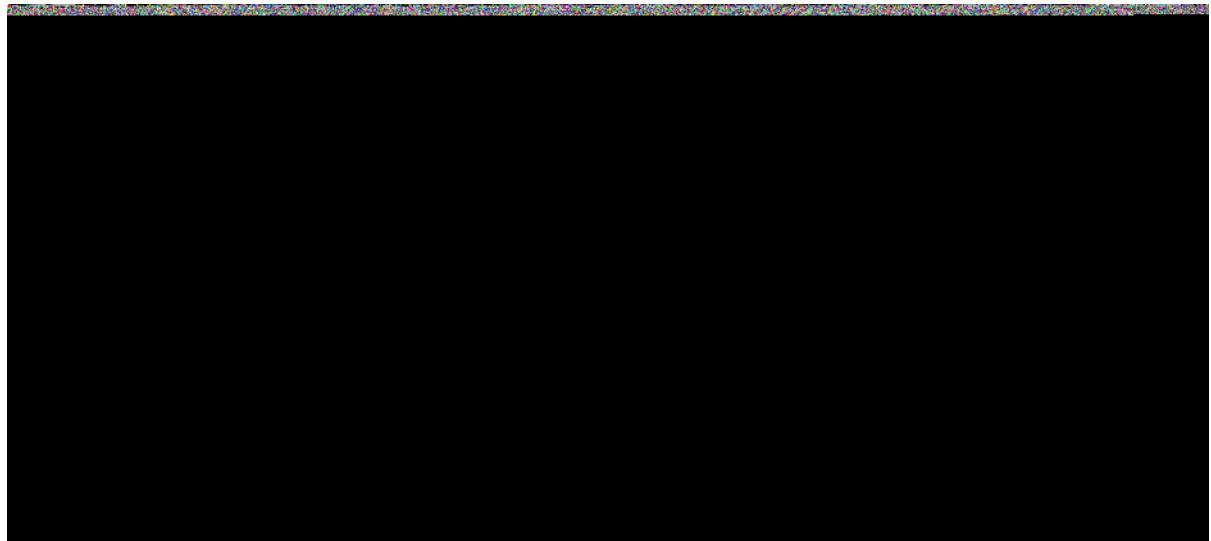
To configure the time-to-live (TTL) value, use the **ttl** command in flow exporter configuration mode. To remove the TTL value, use the **no** form of this command.

```
ttl ttl
no ttl ttl
```

Syntax Description	<i>ttl</i> Time-to-live (TTL) value for exported datagrams. The range is 1 to 255. The default is 255.				
Command Default	Flow exporters use a TTL of 255.				
Command Modes	Flow exporter configuration				
Command History	<table> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	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 **X**

QoS

- [Auto QoS Commands, on page 679](#)
- [QoS Commands, on page 713](#)

Auto QoS Commands

- [auto qos classify](#), on page 679
- [auto qos trust](#), on page 681
- [auto qos video](#), on page 688
- [auto qos voip](#), on page 697
- [debug auto qos](#), on page 710
- [show auto qos](#), on page 711

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 Everest 16.6.1	This command was introduced.

Usage Guidelines	Use this command to configure the QoS for trusted interfaces within the QoS domain. The QoS domain includes the device, the network interior, and edge devices that can classify incoming traffic for QoS.
-------------------------	--

When auto-QoS is enabled, it uses the ingress packet label to categorize traffic, to assign packet labels, and to configure the ingress and egress queues.

Auto-QoS configures the device for connectivity with a trusted interface. The QoS labels of incoming packets are trusted. For nonrouted ports, the CoS value of the incoming packets is trusted. For routed ports, the DSCP value of the incoming packet is trusted.

To take advantage of the auto-QoS defaults, you should enable auto-QoS before you configure other QoS commands. You can fine-tune the auto-QoS configuration *after* you enable auto-QoS.



Note The device applies the auto-QoS-generated commands as if the commands were entered from the command-line interface (CLI). An existing user configuration can cause the application of the generated commands to fail or to be overridden by the generated commands. These actions occur without warning. If all the generated commands are successfully applied, any user-entered configuration that was not overridden remains in the running configuration. Any user-entered configuration that was overridden can be retrieved by reloading the device without saving the current configuration to memory. If the generated commands fail to be applied, the previous running configuration is restored.

After auto-QoS is enabled, do not modify a policy map or aggregate policer that includes *AutoQoS* in its name. If you need to modify the policy map or aggregate policer, make a copy of it, and change the copied policy map or policer. To use the new policy map instead of the generated one, remove the generated policy map from the interface, and apply the new policy map.

To display the QoS configuration that is automatically generated when auto-QoS is enabled, enable debugging before you enable auto-QoS. Use the **debug auto qos** privileged EXEC command to enable auto-QoS debugging.

The following policy maps and class maps are created and applied when running the **auto qos classify** and **auto qos classify police** commands:

Policy maps (For the **auto qos classify police** command):

- AutoQos-4.0-Classify-Police-Input-Policy
- AutoQos-4.0-Output-Policy

Class maps:

- AutoQos-4.0-Multimedia-Conf-Class (match-any)
- AutoQos-4.0-Bulk-Data-Class (match-any)
- AutoQos-4.0-Transaction-Class (match-any)
- AutoQos-4.0-Scavenger-Class (match-any)
- AutoQos-4.0-Signaling-Class (match-any)
- AutoQos-4.0-Default-Class (match-any)
- class-default (match-any)
- AutoQos-4.0-Output-Priority-Queue (match-any)
- AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
- AutoQos-4.0-Output-Trans-Data-Queue (match-any)

- AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
- AutoQos-4.0-Output-Scavenger-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)

To disable auto-QoS on a port, use the **no auto qos classify** interface configuration command. Only the auto-QoS-generated interface configuration commands for this port are removed. If this is the last port on which auto-QoS is enabled and you enter the **no auto qos classify** command, auto-QoS is considered disabled even though the auto-QoS-generated global configuration commands remain (to avoid disrupting traffic on other ports affected by the global configuration).

Examples

This example shows how to enable auto-QoS classification of an untrusted device and police traffic:

You can verify your settings by entering the **show auto qos interface interface-id** privileged EXEC command.

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

Cisco IOS XE Everest
16.6.1

Modification

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 107: Traffic Types, Packet Labels, and Queues

	VOIP Data Traffic	VOIP Control Traffic	Routing Protocol Traffic	STP¹ BPDU² Traffic	Real-Time Video Traffic	All Other Traffic
DSCP ³	46	24, 26	48	56	34	—
CoS ⁴	5	3	6	7	3	—

¹ STP = Spanning Tree Protocol² BPDU = bridge protocol data unit³ DSCP = Differentiated Services Code Point⁴ 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:
```

auto qos trust

```

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

```

auto qos trust

```

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	<table border="1"> <thead> <tr> <th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td><td>This command was introduced.</td></tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				
Usage Guidelines	<p>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.</p> <p>Auto-QoS configures the device for video connectivity to a Cisco TelePresence system, a Cisco IP camera, or a Cisco digital media player.</p> <p>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 <i>after</i> you enable auto-QoS.</p> <p>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</p>				

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 108: Traffic Types, Packet Labels, and Queues

	VOIP Data Traffic	VOIP Control Traffic	Routing Protocol Traffic	STP ⁵ BPDU ⁶ Traffic	Real-Time Video Traffic	All Other Traffic
DSCP ⁷	46	24, 26	48	56	34	—
CoS ⁸	5	3	6	7	3	—

⁵ STP = Spanning Tree Protocol

⁶ BPDU = bridge protocol data unit

⁷ DSCP = Differentiated Services Code Point

⁸ CoS = class of service

Examples

The following is an example of the **auto qos video cts** command and the applied policies and class maps:

```

Device(config)# interface 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 Everest 16.6.1		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 <i>after</i> you enable auto-QoS.
-------------------------	--



Note	The device applies the auto-QoS-generated commands as if the commands were entered from the command-line interface (CLI). An existing user configuration can cause the application of the generated commands to fail or to be overridden by the generated commands. These actions occur without warning. If all the generated commands are successfully applied, any user-entered configuration that was not overridden remains in the running configuration. Any user-entered configuration that was overridden can be retrieved by reloading the device without saving the current configuration to memory. If the generated commands fail to be applied, the previous running configuration is restored.
-------------	---

If this is the first port on which you have enabled auto-QoS, the auto-QoS-generated global configuration commands are executed followed by the interface configuration commands. If you enable auto-QoS on another port, only the auto-QoS-generated interface configuration commands for that port are executed.

When you enter the **auto qos voip cisco-phone** interface configuration command on a port at the edge of the network that is connected to a Cisco IP phone, the device enables the trusted boundary feature. The device uses the Cisco Discovery Protocol (CDP) to detect the presence of a Cisco IP phone. When a Cisco IP phone

is detected, the ingress classification on the port is set to trust the QoS label received in the packet. The device also uses policing to determine whether a packet is in or out of profile and to specify the action on the packet. If the packet does not have a DSCP value of 24, 26, or 46 or is out of profile, the device changes the DSCP value to 0. When a Cisco IP phone is absent, the ingress classification is set to not trust the QoS label in the packet. The policing is applied to those traffic matching the policy-map classification before the device enables the trust boundary feature.

- When you enter the **auto qos voip cisco-softphone** interface configuration command on a port at the edge of the network that is connected to a device running the Cisco SoftPhone, the device uses policing to decide whether a packet is in or out of profile and to specify the action on the packet. If the packet does not have a DSCP value of 24, 26, or 46 or is out of profile, the device changes the DSCP value to 0.
- When you enter the **auto qos voip trust** interface configuration command on a port connected to the network interior, the device trusts the CoS value for nonrouted ports or the DSCP value for routed ports in ingress packets (the assumption is that traffic has already been classified by other edge devices).

You can enable auto-QoS on static, dynamic-access, and voice VLAN access, and trunk ports. When enabling auto-QoS with a Cisco IP phone on a routed port, you must assign a static IP address to the IP phone.



Note

When a device running Cisco SoftPhone is connected to a device or routed port, the device supports only one Cisco SoftPhone application per port.

After auto-QoS is enabled, do not modify a policy map or aggregate policer that includes *AutoQoS* in its name. If you need to modify the policy map or aggregate policer, make a copy of it, and change the copied policy map or policer. To use the new policy map instead of the generated one, remove the generated policy map from the interface, and apply the new policy map.

To display the QoS configuration that is automatically generated when auto-QoS is enabled, enable debugging before you enable auto-QoS. Use the **debug auto qos** privileged EXEC command to enable auto-QoS debugging.

The following policy maps and class maps are created and applied when running the **auto qos voip trust** command:

Policy maps:

- AutoQos-4.0-Trust-Cos-Input-Policy
- AutoQos-4.0-Output-Policy

Class maps:

- class-default (match-any)
- AutoQos-4.0-Output-Priority-Queue (match-any)
- AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
- AutoQos-4.0-Output-Trans-Data-Queue (match-any)
- AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
- AutoQos-4.0-Output-Scavenger-Queue (match-any)

- AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)

The following policy maps and class maps are created and applied when running the **auto qos voip cisco-softphone** command:

Policy maps:

- AutoQos-4.0-CiscoSoftPhone-Input-Policy
- AutoQos-4.0-Output-Policy

Class maps:

- AutoQos-4.0-Voip-Data-Class (match-any)
- AutoQos-4.0-Voip-Signal-Class (match-any)
- AutoQos-4.0-Multimedia-Conf-Class (match-any)
- AutoQos-4.0-Bulk-Data-Class (match-any)
- AutoQos-4.0-Transaction-Class (match-any)
- AutoQos-4.0-Scavenger-Class (match-any)
- AutoQos-4.0-Signaling-Class (match-any)
- AutoQos-4.0-Default-Class (match-any)
- class-default (match-any)
- AutoQos-4.0-Output-Priority-Queue (match-any)
- AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
- AutoQos-4.0-Output-Trans-Data-Queue (match-any)
- AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
- AutoQos-4.0-Output-Scavenger-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)

The following policy maps and class maps are created and applied when running the **auto qos voip cisco-phone** command:

Policy maps:

- service-policy input AutoQos-4.0-CiscoPhone-Input-Policy
- service-policy output AutoQos-4.0-Output-Policy

Class maps:

- class AutoQos-4.0-Voip-Data-CiscoPhone-Class
- class AutoQos-4.0-Voip-Signal-CiscoPhone-Class
- class AutoQos-4.0-Default-Class

To disable auto-QoS on a port, use the **no auto qos voip** interface configuration command. Only the auto-QoS-generated interface configuration commands for this port are removed. If this is the last port on which auto-QoS is enabled and you enter the **no auto qos voip** command, auto-QoS is considered disabled even though the auto-QoS-generated global configuration commands remain (to avoid disrupting traffic on other ports affected by the global configuration).

The device configures egress queues on the port according to the settings in this table.

Table 109: 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

```

auto qos voip

```

    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

```

auto qos voip

```

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 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-Transactional-Class (match-any)
0 packets
Match: access-group name AutoQos-4.0-Acl-Transactional-Data
  0 packets, 0 bytes
  5 minute rate 0 bps
QoS Set
  dscp af21
police:
  cir 10000000 bps, bc 312500 bytes
  conformed 0 bytes; actions:
    transmit
  exceeded 0 bytes; actions:
    set-dscp-transmit dscp table policed-dscp
  conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Scavenger-Class (match-any)
0 packets

```

auto qos voip

```

Match: access-group name AutoQos-4.0-Acl-Scavenger
  0 packets, 0 bytes
  5 minute rate 0 bps
QoS Set
  dscp cs1
police:
  cir 10000000 bps, bc 312500 bytes
  conformed 0 bytes; actions:
    transmit
  exceeded 0 bytes; actions:
    drop
  conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Signaling-Class (match-any)
  0 packets
Match: access-group name AutoQos-4.0-Acl-Signaling
  0 packets, 0 bytes
  5 minute rate 0 bps
QoS Set
  dscp cs3
police:
  cir 32000 bps, bc 8000 bytes
  conformed 0 bytes; actions:
    transmit
  exceeded 0 bytes; actions:
    drop
  conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Default-Class (match-any)
  0 packets
Match: access-group name AutoQos-4.0-Acl-Default
  0 packets, 0 bytes
  5 minute rate 0 bps
QoS Set
  dscp default
police:
  cir 10000000 bps, bc 312500 bytes
  conformed 0 bytes; actions:
    transmit
  exceeded 0 bytes; actions:
    set-dscp-transmit dscp table policed-dscp
  conformed 0000 bps, exceed 0000 bps

Class-map: class-default (match-any)
  0 packets
Match: any
  0 packets, 0 bytes
  5 minute rate 0 bps

Service-policy output: AutoQos-4.0-Output-Policy

queue stats for all priority classes:
  Queueing
  priority level 1

  (total drops) 0
  (bytes output) 0

Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
  0 packets
Match: dscp cs4 (32) cs5 (40) ef (46)
  0 packets, 0 bytes
  5 minute rate 0 bps
Match: cos 5

```

```

    0 packets, 0 bytes
    5 minute rate 0 bps
Priority: 30% (300000 kbps), burst bytes 7500000,
Priority Level: 1

Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
0 packets
Match: dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
    0 packets, 0 bytes
    5 minute rate 0 bps
Match: cos 3
    0 packets, 0 bytes
    5 minute rate 0 bps
Queueing
queue-limit dscp 16 percent 80
queue-limit dscp 24 percent 90
queue-limit dscp 48 percent 100
queue-limit dscp 56 percent 100

(total drops) 0
(bytes output) 0
bandwidth remaining 10%

queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
0 packets
Match: dscp af41 (34) af42 (36) af43 (38)
    0 packets, 0 bytes
    5 minute rate 0 bps
Match: cos 4
    0 packets, 0 bytes
    5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 10%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
0 packets
Match: dscp af21 (18) af22 (20) af23 (22)
    0 packets, 0 bytes
    5 minute rate 0 bps
Match: cos 2
    0 packets, 0 bytes
    5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 10%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
0 packets
Match: dscp af11 (10) af12 (12) af13 (14)
    0 packets, 0 bytes
    5 minute rate 0 bps
Match: cos 1
    0 packets, 0 bytes
    5 minute rate 0 bps

```

debug auto qos

```

Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 4%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
0 packets
Match: dscp cs1 (8)
0 packets, 0 bytes
5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 1%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
0 packets
Match: dscp af31 (26) af32 (28) af33 (30)
0 packets, 0 bytes
5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 10%
queue-buffers ratio 10

Class-map: class-default (match-any)
0 packets
Match: any
0 packets, 0 bytes
5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 25%
queue-buffers ratio 25

```

You can verify your settings by entering the **show auto qos interface *interface-id*** privileged EXEC command.

debug auto qos

To enable debugging of the automatic quality of service (auto-QoS) feature, use the **debug auto qos** command in privileged EXEC mode. Use the **no** form of this command to disable debugging.

```
debug auto qos
no debug auto qos
```

Syntax Description This command has no arguments or keywords.

Command Default Auto-QoS debugging is disabled.

Command Modes	Privileged EXEC	
Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	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 undebbug auto qos command is the same as the no debug auto qos command.	
	When you enable debugging on a device stack, it is enabled only on the active device. To enable debugging on a stack member, you can start a session from the active device by using the session switch-number privileged EXEC command. Then enter the debug command at the command-line prompt of the stack member. You also can use the remote command stack-member-number LINE privileged EXEC command on the active device to enable debugging on a member device without first starting a session.	

Examples

This example shows how to display the QoS configuration that is automatically generated when auto-QoS is enabled:

```
Device# debug auto qos
AutoQoS debugging is on
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# auto qos voip cisco-phone
```

show auto qos

To display the quality of service (QoS) commands entered on the interfaces on which automatic QoS (auto-QoS) is enabled, use the **show auto qos** command in privileged EXEC mode.

show auto qos [interface [interface-id]]

Syntax Description	interface [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 Everest 16.6.1	This command was introduced.

show auto qos

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
```

QoS Commands

- [class](#), on page 713
- [class-map](#), on page 715
- [match \(class-map configuration\)](#), on page 717
- [policy-map](#), on page 719
- [priority](#), on page 721
- [queue-buffers ratio](#), on page 723
- [queue-limit](#), on page 724
- [random-detect cos](#), on page 725
- [random-detect cos-based](#), on page 726
- [random-detect dscp](#), on page 727
- [random-detect dscp-based](#), on page 728
- [random-detect precedence](#), on page 729
- [random-detect precedence-based](#), on page 731
- [service-policy \(Wired\)](#), on page 732
- [set](#), on page 733
- [show class-map](#), on page 738
- [show platform hardware fed active qos](#), on page 739
- [show platform software fed switch qos](#), on page 742
- [show platform software fed switch qos qsb](#), on page 743
- [show policy-map](#), on page 745
- [trust device](#), on page 747

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	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	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. <i>class-map-name</i> The class map name.				
Command Default	No class maps are defined.				
Command Modes	Global configuration Policy map configuration				
Command History	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; padding-bottom: 2px;">Release</th><th style="text-align: left; padding-bottom: 2px;">Modification</th></tr> </thead> <tbody> <tr> <td style="padding-top: 2px;">Cisco IOS XE Everest 16.6.1</td><td style="padding-top: 2px;">This command was introduced.</td></tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				
Usage Guidelines	<p>Use this command to specify the name of the class for which you want to create or modify class-map match criteria and to enter class-map configuration mode.</p> <p>The class-map command and its subcommands are used to define packet classification, marking, and aggregate policing as part of a globally named service policy applied on a per-port basis.</p> <p>After you are in quality of service (QoS) class-map configuration mode, these configuration commands are available:</p> <ul style="list-style-type: none"> • description—Describes the class map (up to 200 characters). The show class-map privileged EXEC command displays the description and the name of the class map. • exit—Exits from QoS class-map configuration mode. • match—Configures classification criteria. • no—Removes a match statement from a class map. <p>If you enter the match-any keyword, you can only use it to specify an extended named access control list (ACL) with the match access-group class-map configuration command.</p> <p>To define packet classification on a physical-port basis, only one match command per class map is supported. The ACL can have multiple access control entries (ACEs).</p>				



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.

match (class-map configuration)

To define the match criteria to classify traffic, use the **match** command in class-map configuration mode. Use the **no** form of this command to remove the match criteria.

```
match {access-group{name acl-name acl-index} | cos cos-value | dscp dscp-value | [ ip ] dscp dscp-list | [ ip ] precedence ip-precedence-list | mpls experimental-value | non-client-nrt | precedence precedence-value1...value4 | protocol protocol-name | qos-group qos-group-value | vlan vlan-id | wlan wlan-id}
no match {access-group{name acl-name acl-index} | cos cos-value | dscp dscp-value | [ ip ] dscp dscp-list | [ ip ] precedence ip-precedence-list | mpls experimental-value | non-client-nrt | precedence precedence-value1...value4 | protocol protocol-name | qos-group qos-group-value | vlan vlan-id | wlan wlan-id}
```

Syntax Description	
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.
<i>acl-index</i>	Specifies the number of an IP standard or extended access control list (ACL) or MAC ACL. For an IP standard ACL, the ACL index range is 1 to 99 and 1300 to 1999. For an IP extended ACL, the ACL index range is 100 to 199 and 2000 to 2699.
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.

match (class-map configuration)

ip precedence <i>ip-precedence-list</i>	Specifies a list of up to eight IP-precedence values to match against incoming packets. Separate each value with a space. The range is 0 to 7. You also can enter a mnemonic name for a commonly used value.
mpls experimental-value	Specifies Multi Protocol Label Switching specific values.
non-client-nrt	Matches a non-client NRT (non-real-time).
precedence <i>precedence-value1...value4</i>	Assigns an IP precedence value to the classified traffic. The range is 0 to 7. You also can enter a mnemonic name for a commonly used value.
protocol <i>protocol-name</i>	Specifies the type of protocol.
qos-group <i>qos-group-value</i>	Identifies a specific QoS group value as a match criterion. The range is 0 to 31.
vlan <i>vlan-id</i>	Identifies a specific VLAN as a match criterion. The range is 1 to 4094.
wlan <i>wlan-id</i>	Identifies 802.11 specific values.

Command Default No match criteria are defined.

Command Modes Class-map configuration

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

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	<i>policy-map-name</i> Name of the policy map.					
Command Default	No policy maps are defined.					
Command Modes	Global configuration (config)					
Command History	<table border="1"> <thead> <tr> <th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td><td>This command was introduced.</td></tr> </tbody> </table>		Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification					
Cisco IOS XE Everest 16.6.1	This command was introduced.					
Usage Guidelines	<p>After entering the policy-map command, you enter policy-map configuration mode, and these configuration commands are available:</p> <ul style="list-style-type: none"> • 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. <p>To return to global configuration mode, use the exit command. To return to privileged EXEC mode, use the end command.</p> <p>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.</p> <p>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.</p> <p>Only one policy map per ingress port is supported. You can apply the same policy map to multiple physical ports.</p> <p>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.</p> <p>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.</p> <p>In VLAN-based QoS, a service policy is applied to an SVI interface.</p>					



Note Not all MQC QoS combinations are supported for wired ports. For information about these restrictions, see chapters "Restrictions for QoS on Wired Targets" in the QoS configuration guide.

Examples

This example shows how to create a policy map called policy1. When attached to the ingress port, it matches all the incoming traffic defined in class1, sets the IP DSCP to 10, and polices the traffic at an average rate of 1 Mb/s and bursts at 20 KB. Traffic less than the profile is sent.

```
Device(config)# policy-map policy1
Device(config-pmap)# class class1
Device(config-pmap-c)# set dscp 10
Device(config-pmap-c)# police 1000000 20000 conform-action transmit
Device(config-pmap-c)# exit
```

This example shows how to configure hierarchical policies:

```
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
Device(config-pmap-c)# end
```

This example shows how to delete a policy map:

```
Device(config)# no policy-map policymap2
```

You can verify your settings by entering the **show policy-map** privileged EXEC command.

priority

To assign priority to a class of traffic belonging to a policy map, use the **priority** command in policy-map class configuration mode. To remove a previously specified priority for a class, use the **no** form of this command.

priority [*Kbps [burst -in-bytes]*] | **level** *level-value* [*Kbps [burst -in-bytes]*] | **percent** *percentage* [*Kb/s [burst -in-bytes]*]

no priority [Kb/s [burst -in-bytes] | level level value [Kb/s [burst -in-bytes]] | percent percentage [Kb/s [burst -in-bytes]]]]

Syntax Description	<i>Kb/s</i>	(Optional) Guaranteed allowed bandwidth, in kilobits per second (kbps), for the priority traffic. The amount of guaranteed bandwidth varies according to the interface and platform in use. Beyond the guaranteed bandwidth, the priority traffic will be dropped in the event of congestion to ensure that the nonpriority traffic is not starved. The value must be between 1 and 2,000,000 kbps.
	<i>burst -in-bytes</i>	(Optional) Burst size in bytes. The burst size configures the network to accommodate temporary bursts of traffic. The default burst value, which is computed as 200 milliseconds of traffic at the configured bandwidth rate, is used when the burst argument is not specified. The range of the burst is from 32 to 2000000 bytes.
	level <i>level-value</i>	(Optional) Assigns priority level. Available values for <i>level-value</i> are 1 and 2. Level 1 is a higher priority than Level 2. Level 1 reserves bandwidth and goes first, so latency is very low.
	percent <i>percentage</i>	(Optional) Specifies the amount of guaranteed bandwidth to be specified by the percent of available bandwidth.

Command Default	No priority is set.				
Command Modes	Policy-map class configuration (config-pmap-c)				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	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	<i>ratio limit</i> (Optional) Configures the queue buffer for the class. Enter the queue buffers ratio limit (0-100).				
Command Default	No queue buffer for the class is defined.				
Command Modes	Policy-map class configuration (config-pmap-c)				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				

Usage Guidelines Either the **bandwidth**, **shape**, or **priority** command must be used before using this command. For more information about these commands, see *Cisco IOS Quality of Service Solutions Command Reference* available on Cisco.com

The allows you to allocate buffers to queues. If buffers are not allocated, then they are divided equally amongst all queues. You can use the queue-buffer ratio to divide it in a particular ratio. The buffers are soft buffers because Dynamic Threshold and Scaling (DTS) is active on all queues by default.

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

```

queue-limit

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	<p>queue-limit-size</p> <p>cos cos-value</p> <p>dscp dscp-value</p> <p>percent percentage-of-packets</p>	<p>The maximum size of the queue. The maximum varies according to the optional unit of measure keyword specified (bytes, ms, us, or packets).</p> <p>Specifies parameters for each cos value. CoS values are from 0 to 7.</p> <p>Specifies parameters for each DSCP value.</p> <p>You can specify a value in the range 0 to 63 specifying the differentiated services code point value for the type of queue limit .</p> <p>A percentage in the range 1 to 100 specifying the maximum percentage of packets that the queue for this class can accumulate.</p>
Command Default	None	
Command Modes	Policy-map class configuration (policy-map-c)	
Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1 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	<i>cos-value</i>	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.
	<i>percent</i>	Specifies that the minimum and threshold values are in percentage.
	<i>min-threshold</i>	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.
	<i>max-threshold</i>	Maximum threshold in number of packets. The value range of this argument is from the value of the <i>min-threshold</i> 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 Everest 16.6.1	This command was introduced.

random-detect cos-based**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
show queueing	Lists all or selected configured queueing strategies.

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 Everest 16.6.1	This command was introduced.

Examples

In the following example, WRED is configured on the basis of the CoS value.

```
Switch> enable
Switch# configure terminal
Switch(config)# policy-map policymap1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# random-detect cos-based
Switch(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	<i>dscp-value</i>	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 .
	<i>percent</i>	Specifies that the minimum and threshold values are in percentage.
	<i>min-threshold</i>	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.
	<i>max-threshold</i>	Maximum threshold in number of packets. The value range of this argument is from the value of the <i>min-threshold</i> 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 Everest 16.6.1	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.

random-detect dscp-based

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
show queueing	Lists all or selected configured queueing strategies.

random-detect dscp-based

To base weighted random early detection (WRED) on the Differentiated Services Code Point (dscp) value of a packet, use the **random-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 Everest 16.6.1	This command was introduced.

Usage GuidelinesWith 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:

```

Switch> enable
Switch# configure terminal
Switch(config)#
policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# bandwidth percent 80
Switch(config-pmap-c)# random-detect dscp-based
Switch(config-pmap-c)# random-detect dscp 2 percent 10 40
Switch(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

<i>precedence</i>	IP precedence number. The value range is from 0 to 7; see Table 1 in the “Usage Guidelines” section.
<i>percent</i>	Indicates that the threshold values are in percentage.
<i>min-threshold</i>	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.

random-detect precedence

<i>max-threshold</i>	Maximum threshold in number of packets. The value range of this argument is from the value of the <i>min-threshold</i> 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)

Release	Modification
Cisco IOS XE Everest 16.6.1	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 Everest 16.6.1		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
```

service-policy (Wired)

```
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 Everest 16.6.1	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	<p>Sets the Layer 2 class of service (CoS) value or user priority of an outgoing packet. You can specify these values:</p> <ul style="list-style-type: none"> • <i>cos-value</i>—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: <ul style="list-style-type: none"> • 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 <i>table-map-name</i>—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. <p>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.</p>

dscp	<p>Sets the differentiated services code point (DSCP) value to mark IP(v4) and IPv6 packets. You can specify these values:</p> <ul style="list-style-type: none"> • <i>cos-value</i>—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: <ul style="list-style-type: none"> • 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 <i>table-map-name</i>—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. <p>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.</p>
ip	<p>Sets IP values to the classified traffic. You can specify these values:</p> <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none">• 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.<ul style="list-style-type: none">• 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 <i>table-map-name</i>—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	<p>Assigns a QoS group identifier that can be used later to classify packets.</p> <ul style="list-style-type: none"> • <i>qos-group-value</i>—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 <i>table-map-name</i>—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. <p>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.</p>
------------------	---

Command Default	No traffic classification is defined.
------------------------	---------------------------------------

Command Modes	Policy-map class configuration
----------------------	--------------------------------

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

The **cos**, **dscp**, **qos-group**, **wlantable**, *table-map-name*, keywords were added.

Usage Guidelines	For the set dscp dscp-value command, the set cos cos-value command, and the set ip precedence precedence-value command, you can enter a mnemonic name for a commonly used value. For example, you can enter the set dscp af11 command, which is the same as entering the set dscp 10 command. You can enter the set ip precedence critical command, which is the same as entering the set ip precedence 5 command. For a list of supported mnemonics, enter the set dscp ? or the set ip precedence ? command to see the command-line help strings.
-------------------------	--

When you configure the **set dscp cos** command, note the following: The CoS value is a 3-bit field, and the DSCP value is a 6-bit field. Only the three bits of the CoS field are used.

When you configure the **set dscp qos-group** command, note the following:

- The valid range for the DSCP value is a number from 0 to 63. The valid value range for the QoS group is a number from 0 to 99.

show class-map

- If a QoS group value falls within both value ranges (for example, 44), the packet-marking value is copied and the packets is marked.
- If QoS group value exceeds the DSCP range (for example, 77), the packet-marking value is not be copied and the packet is not marked. No action is taken.

The **set qos-group** command cannot be applied until you create a service policy in policy-map configuration mode and then attach the service policy to an interface or ATM virtual circuit (VC).

To return to policy-map configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

Examples

This example shows how to assign DSCP 10 to all FTP traffic without any policers:

```
Device(config)# policy-map policy_ftp
Device(config-pmap)# class-map ftp_class
Device(config-cmap)# exit
Device(config)# policy policy_ftp
Device(config-pmap)# class ftp_class
Device(config-pmap-c)# set dscp 10
Device(config-pmap) # exit
```

You can verify your settings by entering the **show policy-map** privileged EXEC command.

show class-map

To display quality of service (QoS) class maps, which define the match criteria to classify traffic, use the **show class-map** command in EXEC mode.

show class-map [class-map-name | type control subscriber {all | class-map-name}]

Syntax Description

class-map-name (Optional) Class map name.

type control subscriber (Optional) Displays information about control class maps.

all (Optional) Displays information about all control class maps.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced.

This is an example of output from the **show class-map** command:

```
Device# show class-map
Class Map match-any videowizard_10-10-10-10 (id 2)
  Match access-group name videowizard_10-10-10-10
```

Examples

```

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 active qos

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

This topic elaborates only the QoS-specific options, that is, the options available with the **show platform hardware fed {active | standby} qos** command.

```

show platform hardware fed {active | standby} qos {afd | {config type type | [{asic asic_num}] | stats
clients {all | bssid 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}] | {asicnumber} | stats | {iifd_id id | interface type number | internal {cpu
policer | port-type type asic number} {asicnumber [{port_num}]} } } | resource}

```

Syntax Description

{active | standby } Switch for which you want to display information. You have the following options:

- **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.

af~~d~~ {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

stats client :

- **all**—Displays statistics of all client.
- **bssid**—Valid range is from 1 to 4294967295.

asicasic_num

(Optional) ASIC number. Valid range is from 0 to 255.

show platform hardware fed active qos

dscp-cos counters { Displays per port dscp-cos counters. You must choose from the following options
iifd_id id | interface under **dscp-cos counters:**
type number }

- **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 **leinfo**:

- **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 Everest 16.6.1	This command was introduced.

This is an example of output from the **show platform hardware fed active qos queue stats internal cpu policer** command

```
Device# show platform hardware fed active qos queue stats internal cpu policer
```

CPU Queue Statistics							
QId	PlcIdx	Queue Name	Enabled	(default)	(set)	Queue	
				Rate	Rate	Drop (Bytes)	
Drop (Frames)							
0	11	DOT1X Auth	Yes	1000	1000	0	0
1	1	L2 Control	Yes	2000	400	0	0
2	14	Forus traffic	Yes	4000	1000	0	0
3	0	ICMP GEN	Yes	600	200	0	0
4	2	Routing Control	Yes	5400	1800	0	0
5	14	Forus Address resolution	Yes	4000	1000	0	0
6	0	ICMP Redirect	Yes	600	200	0	0
7	16	Inter FED Traffic	Yes	2000	1000	0	0
8	4	L2 LVX Cont Pack	Yes	1000	1000	0	0
9	16	EWLC Control	Yes	2000	1000	0	0
10	16	EWLC Data	Yes	2000	1000	0	0
11	13	L2 LVX Data Pack	Yes	1000	1000	0	0
12	0	BROADCAST	Yes	600	200	0	0
13	10	Learning cache ovfl	Yes	100	200	0	0
14	13	Sw forwarding	Yes	1000	1000	0	0
15	8	Topology Control	Yes	13000	13000	0	0
16	12	Proto Snooping	Yes	2000	400	0	0
17	6	DHCP Snooping	No	500	400	0	0
18	9	Transit Traffic	Yes	500	400	0	0
19	10	RPF Failed	Yes	100	200	0	0
20	15	MCAST END STATION	Yes	2000	2000	0	0
21	13	LOGGING	Yes	1000	1000	0	0
22	7	Punt Webauth	Yes	1000	1000	0	0
23	10	Crypto Control	Yes	100	200	0	0
24	10	Exception	Yes	100	200	0	0
25	3	General Punt	Yes	200	200	0	0
26	10	NFL SAMPLED DATA	Yes	100	200	0	0
27	2	Low Latency	Yes	5400	1800	0	0
28	10	EGR Exception	Yes	100	200	0	0
29	5	Stackwise Virtual Control	No	8000	8000	0	0
30	9	MCAST Data	Yes	500	400	0	0
31	10	Gold Pkt	Yes	100	200	0	0

* NOTE: CPU queue policer rates are configured to the closest hardware supported value

CPU Queue Policer Statistics				
Policer Index	Policer Accept Bytes	Policer Accept Frames	Policer Drop Bytes	Policer Drop Frames
0	0	0	0	0
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0

show platform software fed switch qos

```

8      0      0      0      0
9      0      0      0      0
10     10336   152    0      0
11     0      0      0      0
12     0      0      0      0
13     0      0      0      0
14     0      0      0      0
15     0      0      0      0
16     0      0      0      0
17     0      0      0      0

CPP Classes to queue map
=====
PlcIdx CPP Class : Queues
-----
0  system-cpp-police-data : ICMP GEN/BROADCAST/ICMP Redirect/
10 system-cpp-police-sys-data : Learning cache ovfl/Crypto
Control/Exception/EGR Exception/NFL SAMPLED DATA/Gold Pkt/RPF Failed/
13 system-cpp-police-sw-forward : Sw forwarding/LOGGING/L2 LVX Data Pack/
9  system-cpp-police-multicast : Transit Traffic/MCAST Data/
15 system-cpp-police-multicast-end-station : MCAST END STATION /
7   system-cpp-police-punt-weauth : Punt Webauth/
1  system-cpp-police-l2-control : L2 Control/
2  system-cpp-police-routing-control : Routing Control/Low Latency/
3   system-cpp-police-control-low-priority : General Punt/
4   system-cpp-police-l2lvx-control : L2 LVX Cont Pack/
8   system-cpp-police-topology-control : Topology Control/
11  system-cpp-police-dot1x-auth : DOT1X Auth/
12  system-cpp-police-protocol-snooping : Proto Snooping/
6   system-cpp-police-dhcp-snooping : DHCP Snooping/
14  system-cpp-police-forus : Forus Address resolution/Forus traffic/
5   system-cpp-police-stackwise-virt-control : Stackwise Virtual Control/
16  system-cpp-default : Inter FED Traffic/EWLC Control/EWLC Data/
Device#

```

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 {avc | internal | label2qmap | nflqos | policer | policy | qsb | tablemap}** command.

show platform software fed switch{*switch number* | active | standby} qos {avc | internal | label2qmap | nflqos | policer | policy | qsb | tablemap}

Syntax Description

switch {<i>switch_num</i>	The device for which you want to display information.
 active standby	<ul style="list-style-type: none"> • <i>switch_num</i>—Enter the switch ID. Displays information for the specified switch. • active—Displays information for the active switch. • standby—Displays information for the standby switch, if available.

qos	Displays QoS software information. Choose one the following options: <ul style="list-style-type: none">• 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 Everest 16.6.1	This command was introduced.

show platform software fed switch qos qsb

To display QoS sub-block information, use the **show platform software fed switch *switch_number* qos qsb** command.

```
show platform software fed switch{switch number | active | standby} qosqsb {brief | [{all | type | {clientclient_id | port port_number | radioradio_type | ssidssid}}]} | iif_ifid | interface | {Auto-Templateinterface_number | BDIinterface_number | Capwapinterface_number | GigabitEthernetinterface_number | InternalInterfaceinterface_number | Loopbackinterface_number | Nullinterface_number | Port-channelinterface_number | TenGigabitEthernetinterface_number | Tunnelinterface_number | Vlaninterface_number}}
```

Syntax Description	switch The switch for which you want to display information. { <i>switch_num</i> active standby • <i>switch_num</i> —Enter the ID of the switch. Displays information for the specified switch. } • active —Displays information for the active switch. • standby —Displays information for the standby switch, if available.
qos qsb	Displays QoS sub-block software information.

show platform software fed switch qos qsb

**qsb {brief | iif_id | brief
interface}**

- **all**—Displays information for all client.
- **type**—Displays qsb information for the specified target type:
 - **client**—Displays QoS qsb information for wireless clients
 - **port**—Displays port-specific information
 - **radio**—Displays QoS qsb information for wireless radios
 - **ssid**—Displays QoS qsb information for wireless networks

iif_id—Displays information for the iif_ID

interface—Displays QoS qsb information for the specified interface:

- **Auto-Template**—Auto-template interface between 1 and 999.
- **BDI**—Bridge-domain interface between 1 and 16000.
- **Capwap**—CAPWAP interface between 0 and 2147483647.
- **GigabitEthernet**—GigabitEthernet interface between 0 and 9.
- **InternalInterface**—Internal interface between 0 and 9.
- **Loopback**—Loopback interface between 0 and 2147483647.
- **Null**—Null interface 0-0
- **Port-Channel**—Port-channel interface between 1 and 128.
- **TenGigabitEthernet**—TenGigabitEthernet interface between 0 and 9.
- **Tunnel**—Tunnel interface between 0 and 2147483647.
- **Vlan**—VLAN interface between 1 and 4094.

Command Modes User EXEC

Privileged EXEC

Command History Cisco IOS XE Everest 16.6.1 This command was introduced.

This is an example of the output for the **show platform software fed switch switch_number qos qsb** command

```
Device#sh pl so fed sw 3 qos qsb interface g3/0/2

QoS subblock information:
Name:GigabitEthernet3/0/2 iif_id:0x0000000000007b iif_type:ETHER(146)
qsb_ptr:0xffffd8573350
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:::{(0xffffd8685180,AutoQos-4.0-CiscoPhone-Input-Policy,1083231504,)}
    tcg:{0xffffd867ad10,GigabitEthernet3/0/2 tgt(0x7b,IN) level:0 num_tccg:4 num_child:0},
  status:VALID,SET_INHW
  Egress Policy: pmap:::{(0xffffd86857d0,AutoQos-4.0-Output-Policy,1076629088,)}
    tcg:{0xffffd8685b40,GigabitEthernet3/0/2 tgt(0x7b,OUT) level:0 num_tccg:8 num_child:0},
  status:VALID,SET_INHW
  TCG(in,out):(0xffffd867ad10, 0xffffd8685b40) 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}

show policy-map type control subscriber detail

Syntax Description

policy-map-name	(Optional) Name of the policy-map.
interface interface-id	(Optional) Displays the statistics and the configurations of the input and output policies that are attached to the interface.
type control subscriber detail	(Optional) Identifies the type of QoS policy and the statistics.

Command Modes

User EXEC

Privileged EXEC

show policy-map

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.
Usage Guidelines	Policy maps can include policers that specify the bandwidth limitations and the action to take if the limits are exceeded.	
Note	Though visible in the command-line help string, the control-plane , session , and type keywords are not supported, and the statistics shown in the display should be ignored.	

This is an example of the output for the **show policy-map interface** command.

```
Device# show policy-map interface gigabitethernet1/0/48GigabitEthernet1/0/48
Service-policy output: port_shape_parent
Class-map: class-default (match-any)
 191509734 packets
 Match: any
 Queueing
  (total drops) 524940551420
  (bytes output) 14937264500
  shape (average) cir 250000000, bc 2500000, be 2500000
  target shape rate 250000000
Service-policy : child_trip_play
  queue stats for all priority classes:
    Queueing
    priority level 1
    (total drops) 524940551420
    (bytes output) 14937180648
  queue stats for all priority classes:
    Queueing
    priority level 2
    (total drops) 0
    (bytes output) 0
Class-map: dscp56 (match-any)
  191508445 packets
  Match: dscp cs7 (56)
  0 packets, 0 bytes
  5 minute rate 0 bps
  Priority: Strict,
Priority Level: 1
police:
  cir 10 %
  cir 25000000 bps, bc 781250 bytes
  conformed 0 bytes; actions: >>>>counters not supported
  transmit
  exceeded 0 bytes; actions:
    drop
  conformed 0000 bps, exceeded 0000 bps >>>>counters not supported
```

trust device

To configure trust for supported devices connected to an interface, use the **trust device** command in interface configuration mode. Use the **no** form of this command to disable trust for the connected device.

```
trust device {cisco-phone | cts | ip-camera | media-player}
no trust device {cisco-phone | cts | ip-camera | media-player}
```

Syntax Description	cisco-phone Configures a Cisco IP phone cts Configures a Cisco TelePresence System ip-camera Configures an IP Video Surveillance Camera (IPVSC) media-player Configures a Cisco Digital Media Player (DMP)				
Command Default	Trust disabled				
Command Modes	Interface configuration				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	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 XI

Routing

- Bidirectional Forwarding Detection Commands, on page 751
- IP Routing Commands, on page 763

CHAPTER 10

Bidirectional Forwarding Detection Commands

- authentication (BFD), on page 751
- bfd, on page 752
- bfd all-interfaces, on page 753
- bfd check-ctrl-plane-failure, on page 754
- bfd echo, on page 755
- bfd slow-timers, on page 756
- bfd template, on page 757
- bfd-template single-hop, on page 757
- ip route static bfd, on page 758
- ipv6 route static bfd, on page 760

authentication (BFD)

To configure authentication in a Bidirectional Forwarding Detection (BFD) template for single hop sessions, use the **authentication** command in BFD configuration mode. To disable authentication in BFD template for single-hop sessions, use the **no** form of this command

```
authentication authentication-type keychain keychain-name  
no authentication authentication-type keychain keychain-name
```

Syntax Description	<i>authentication-type</i> Authentication type. Valid values are md5, meticulous-md5, meticulous-sha1, and sha-1. <i>keychain keychain-name</i> Configures an authentication key chain with the specified name. The maximum number of characters allowed in the name is 32.
Command Default	Authentication in BFD template for single hop sessions is not enabled.
Command Modes	BFD configuration (config-bfd)
Command History	Release Modification 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-value argument is from 3 to 50.

Command Default

No baseline BFD session parameters are set.

Command Modes

Interface configuration (config-if)

Command History**Release Modification**

This command was introduced.

Usage Guidelines

The **bfd** command can be configured on SVI, Ethernet and port-channel interfaces.

If BFD runs on a port channel interface, BFD has a timer value restriction of $250 * 3$ milliseconds.

The **bfd** interval configuration is not removed when:

- an IPv4 address is removed from an interface
- an IPv6 address is removed from an interface

- IPv6 is disabled from an interface
- an interface is shutdown
- IPv4 CEF is disabled globally or locally on an interface
- IPv6 CEF is disabled globally or locally on an interface

The bfd interval configuration is removed when the subinterface on which its is configured is removed.



Note If we configure bfd interval command in interface config mode, then bfd echo mode is enabled by default. We need to enable either no ip redirect (if BFD echo is needed) or no bfd echo in interface config mode.

Before using BFD echo mode, you must disable sending Internet Control Message Protocol (ICMP) redirect messages by entering the no ip redirect command, in order to avoid high CPU utilization.

Examples

The following example shows the BFD session parameters set for Gigabit Ethernet 1/0/3:

```
Device> enable
Device# configuration terminal
Device(config)# interface gigabitethernet 1/0/3
Device(config-if)# bfd interval 100 min_rx 100 multiplier 3
```

bfd all-interfaces

To enable Bidirectional Forwarding Detection (BFD) for all interfaces participating in the routing process, use the **bfd all-interfaces** command in router configuration or address family interface configuration mode. To disable BFD for all neighbors on a single interface, use the **no** form of this command

bfd all-interfaces
no bfd all-interfaces

Syntax Description

This command has no arguments or keywords.

Command Default

BFD is disabled on the interfaces participating in the routing process.

Command Modes

Router configuration (config-router)

Command History

Release Modification

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
```

bfd check-ctrl-plane-failure

```
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**

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**

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
```

bfd slow-timers

```

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**

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**

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.

ip route static bfd

template-name Template name.

Command Default A BFD template does not exist.

Command Modes Global configuration (config)

Command History **Release Modification**

This command was introduced.

Usage Guidelines The **bfd-template** command allows you to create a BFD template and places the device in BFD configuration mode. The template can be used to specify a set of BFD interval values. BFD interval values specified as part of the BFD template are not specific to a single interface.

Examples The following example shows how to create a BFD template and specify BFD interval values:

```
Device> enable
Device# configuration terminal
Device(config)# bfd-template single-hop node1
Device(bfd-config) #interval min-tx 100 min-rx 100 multiplier 3
Device(bfd-config) #echo
```

The following example shows how to create a BFD single-hop template and configure BFD interval values and an authentication key chain:

```
Device> enable
Device# configuration terminal
Device(config)# bfd-template single-hop template1
Device(bfd-config) #interval min-tx 200 min-rx 200 multiplier 3
Device(bfd-config) #authentication keyed-sha-1 keychain bfd_singlehop
```



Note BFD echo is not enabled by default in the **bfd-template** configuration. This needs to be configured explicitly.

ip route static bfd

To specify static route bidirectional forwarding detection (BFD) neighbors, use the **ip route static bfd** command in global configuration mode. To remove a static route BFD neighbor, use the **no** form of this command

```
ip route static bfd {interface-type interface-number ip-address | vrf vrf-name} [group group-name]
[passive] [unassociate]
no ip route static bfd {interface-type interface-number ip-address | vrf vrf-name} [group group-name]
[passive] [unassociate]
```

Syntax Description

interface-type interface-number

Interface type and number.

<i>ip-address</i>	IP address of the gateway, in A.B.C.D format.
vrf <i>vrf-name</i>	Specifies Virtual Routing and Forwarding (VRF) instance and the destination vrf name.
group <i>group-name</i>	(Optional) Assigns a BFD group. The group-name is a character string of up to 32 characters specifying the BFD group name.
unassociate	(Optional) Unassociates the static route configured for a BFD.

Command Default No static route BFD neighbors are specified.

Command Modes Global configuration (config)

Command History

Release Modification

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

ipv6 route static bfd

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	<p>vrf vrf-name</p> <p>(Optional) Name of the virtual routing and forwarding (VRF) instance by which static routes should be specified.</p>
	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	<p>Release Modification</p> <p>This command was introduced.</p>

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
```

```
■ ipv6 route static bfd
```

IP Routing Commands

- [aggregate-address](#), on page 764
- [area nssa](#), on page 767
- [area virtual-link](#), on page 768
- [auto-summary \(BGP\)](#), on page 771
- [bgp graceful-restart](#), on page 773
- [clear proximity ip bgp](#), on page 775
- [default-information originate \(OSPF\)](#), on page 779
- [default-metric \(BGP\)](#), on page 780
- [distance \(OSPF\)](#), on page 782
- [eigrp log-neighbor-changes](#), on page 784
- [ip authentication key-chain eigrp](#), on page 785
- [ip authentication mode eigrp](#), on page 786
- [ip bandwidth-percent eigrp](#), on page 787
- [ip cef load-sharing algorithm](#), on page 788
- [ip community-list](#), on page 789
- [ip prefix-list](#), on page 793
- [ip hello-interval eigrp](#), on page 796
- [ip hold-time eigrp](#), on page 797
- [ip load-sharing](#), on page 798
- [ip ospf database-filter all out](#), on page 799
- [ip ospf name-lookup](#), on page 800
- [ip split-horizon eigrp](#), on page 800
- [ip summary-address eigrp](#), on page 801
- [metric weights \(EIGRP\)](#), on page 803
- [neighbor advertisement-interval](#), on page 805
- [neighbor default-originate](#), on page 806
- [neighbor description](#), on page 808
- [neighbor ebgp-multihop](#), on page 809
- [neighbor maximum-prefix \(BGP\)](#), on page 810
- [neighbor peer-group \(assigning members\)](#), on page 812
- [neighbor peer-group \(creating\)](#), on page 813
- [neighbor route-map](#), on page 816
- [neighbor update-source](#), on page 817

aggregate-address

- [network \(BGP and multiprotocol BGP\)](#), on page 819
- [network \(EIGRP\)](#), on page 821
- [nsf \(EIGRP\)](#), on page 822
- [offset-list \(EIGRP\)](#), on page 823
- [redistribute \(IP\)](#), on page 824
- [router-id](#), on page 832
- [router bgp](#), on page 833
- [router eigrp](#), on page 836
- [router ospf](#), on page 836
- [set community](#), on page 837
- [set ip next-hop \(BGP\)](#), on page 839
- [show ip bgp](#), on page 841
- [show ip bgp neighbors](#), on page 852
- [show ip eigrp interfaces](#), on page 871
- [show ip eigrp neighbors](#), on page 874
- [show ip eigrp topology](#), on page 876
- [show ip eigrp traffic](#), on page 881
- [show ip ospf](#), on page 882
- [show ip ospf border-routers](#), on page 889
- [show ip ospf database](#), on page 890
- [show ip ospf interface](#), on page 899
- [show ip ospf neighbor](#), on page 902
- [show ip ospf virtual-links](#), on page 907
- [summary-address \(OSPF\)](#), on page 908
- [timers throttle spf](#), on page 909

aggregate-address

To create an aggregate entry in a Border Gateway Protocol (BGP) database, use the **aggregate-address** command in address family or router configuration mode. To disable this function, use the **no** form of this command.

```
aggregate-address address mask [as-set] [as-confed-set] [summary-only] [suppress-map map-name]
[advertise-map map-name] [attribute-map map-name]
no aggregate-address address mask [as-set] [as-confed-set] [summary-only] [suppress-map
map-name] [advertise-map map-name] [attribute-map map-name]
```

Syntax Description	
address	Aggregate address.
mask	Aggregate mask.
as-set	(Optional) Generates autonomous system set path information.
as-confed-set	(Optional) Generates autonomous confederation set path information.
summary-only	(Optional) Filters all more-specific routes from updates.

suppress-map <i>map-name</i>	(Optional) Specifies the name of the route map used to select the routes to be suppressed.
advertise-map <i>map-name</i>	(Optional) Specifies the name of the route map used to select the routes to create AS_SET origin communities.
attribute-map <i>map-name</i>	(Optional) Specifies the name of the route map used to set the attribute of the aggregate route.

Command Default The atomic aggregate attribute is set automatically when an aggregate route is created with this command unless the **as-set** keyword is specified.

Command Modes Address family configuration (config-router-af)
Router configuration (config-router)

Table 110:

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines You can implement aggregate routing in BGP and Multiprotocol BGP (mBGP) either by redistributing an aggregate route into BGP or mBGP, or by using the conditional aggregate routing feature.

Using the **aggregate-address** command with no keywords will create an aggregate entry in the BGP or mBGP routing table if any more-specific BGP or mBGP routes are available that fall within the specified range. (A longer prefix that matches the aggregate must exist in the Routing Information Base (RIB).) The aggregate route will be advertised as coming from your autonomous system and will have the atomic aggregate attribute set to show that information might be missing. (By default, the atomic aggregate attribute is set unless you specify the **as-set** keyword.)

Using the **as-set** keyword creates an aggregate entry using the same rules that the command follows without this keyword, but the path advertised for this route will be an AS_SET consisting of all elements contained in all paths that are being summarized. Do not use this form of the **aggregate-address** command when aggregating many paths, because this route must be continually withdrawn and updated as autonomous system path reachability information for the summarized routes changes.

Using the **as-confed-set** keyword creates an aggregate entry using the same rules that the command follows without this keyword. This keyword performs the same function as the **as-set** keyword, except that it generates autonomous confed set path information.

Using the **summary-only** keyword not only creates the aggregate route (for example, 192.*.*.*) but also suppresses advertisements of more-specific routes to all neighbors. If you want to suppress only advertisements to certain neighbors, you may use the **neighbor distribute-list** command, with caution. If a more-specific route leaks out, all BGP or mBGP routers will prefer that route over the less-specific aggregate you are generating (using longest-match routing).

Using the **suppress-map** keyword creates the aggregate route but suppresses advertisement of specified routes. You can use the **match** clauses of route maps to selectively suppress some more-specific routes of the aggregate and leave others unsuppressed. IP access lists and autonomous system path access lists match clauses are supported.

aggregate-address

Using the **advertise-map** keyword selects specific routes that will be used to build different components of the aggregate route, such as AS_SET or community. This form of the **aggregate-address** command is useful when the components of an aggregate are in separate autonomous systems and you want to create an aggregate with AS_SET, and advertise it back to some of the same autonomous systems. You must remember to omit the specific autonomous system numbers from the AS_SET to prevent the aggregate from being dropped by the BGP loop detection mechanism at the receiving router. IP access lists and autonomous system path access lists **match** clauses are supported.

Using the **attribute-map** keyword allows attributes of the aggregate route to be changed. This form of the **aggregate-address** command is useful when one of the routes forming the AS_SET is configured with an attribute such as the community no-export attribute, which would prevent the aggregate route from being exported. An attribute map route map can be created to change the aggregate attributes.

AS-Set Example

In the following example, an aggregate BGP address is created in router configuration mode. The path advertised for this route will be an AS_SET consisting of all elements contained in all paths that are being summarized.

```
Device(config)#router bgp 50000
Device(config-router)#aggregate-address 10.0.0.0 255.0.0.0 as-set
```

Summary-Only Example

In the following example, an aggregate BGP address is created in address family configuration mode and applied to the multicast database under the IP Version 4 address family. Because the **summary-only** keyword is configured, more-specific routes are filtered from updates.

```
Device(config)#router bgp 50000
Device(config-router)#address-family ipv4 multicast
Device(config-router-af)#aggregate-address 10.0.0.0 255.0.0.0 summary-only
```

Conditional Aggregation Example

In the following example, a route map called MAP-ONE is created to match on an AS-path access list. The path advertised for this route will be an AS_SET consisting of elements contained in paths that are matched in the route map.

```
Device(config)#ip as-path access-list 1 deny ^1234_
Device(config)#ip as-path access-list 1 permit .*
Device(config)#
Device(config)#route-map MAP-ONE
Device(config-route-map)#match ip as-path 1
Device(config-route-map)#exit
Device(config)#router bgp 50000
Device(config-router)#address-family ipv4
Device(config-router-af)#aggregate-address 10.0.0.0 255.0.0.0 as-set advertise-map
MAP-ONE
Router(config-router-af)#end
```

Related Commands	Command	Description
	address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
	ip as-path access-list	Defines a BGP autonomous system path access list.
	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 distribute-list	Distributes BGP neighbor information in an access list.
	route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.

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 [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.

area virtual-link

Command Modes Router address family topology configuration (config-router-af-topology) Router configuration (config-router)

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	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:**

<i>area-id</i>	Area ID assigned to the virtual link. This can be either a decimal value or a valid IPv6 prefix. There is no default.
<i>router-id</i>	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.
<i>chain-name</i>	Name of the authentication key that is valid.
hello-interval <i>seconds</i>	(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 <i>seconds</i>	(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 <i>seconds</i>	(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 <i>seconds</i>	(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 <i>hop-count</i>	(Optional) Configures Time-to-Live (TTL) security on a virtual link. The <i>hop-count</i> 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 Everest 16.6.1	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:

```
ipv6 router ospf 1
log-adjacency-changes
area 1 virtual-link 192.168.255.1
```

The following example establishes a virtual link in OSPF for IPv6:

```
ipv6 router ospf 1
log-adjacency-changes
area 1 virtual-link 192.168.255.1 hello-interval 5
```

The following example shows how to configure TTL security for a virtual link in OSPFv3 for IPv6:

```
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:

```
area 1 virtual-link 1.1.1.1 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.

auto-summary (BGP)

To configure automatic summarization of subnet routes into network-level routes, use the **auto-summary** command in address family or router configuration mode. To disable automatic summarization and send subprefix routing information across classful network boundaries, use the **no** form of this command.

auto-summary
no auto-summary

Syntax Description This command has no arguments or keywords.

Command Default Automatic summarization is disabled by default (the software sends subprefix routing information across classful network boundaries).

Command Modes Address family configuration (config-router-af)
 Router configuration (config-router)

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines BGP automatically summarizes routes to classful network boundaries when this command is enabled. Route summarization is used to reduce the amount of routing information in routing tables. Automatic summarization applies to connected, static, and redistributed routes.



Note The MPLS VPN Per VRF Label feature does not support auto-summary.

By default, automatic summarization is disabled and BGP accepts subnets redistributed from an Interior Gateway Protocol (IGP). To block subnets and create summary subprefixes to the classful network boundary when crossing classful network boundaries, use the **auto-summary** command.

To advertise and carry subnet routes in BGP when automatic summarization is enabled, use an explicit **network** command to advertise the subnet. The **auto-summary** command does not apply to routes injected into BGP via the **network** command or through iBGP or eBGP.

Why auto-summary for BGP Is Disabled By Default

When **auto-summary** is enabled, routes injected into BGP via redistribution are summarized on a classful boundary. Remember that a 32-bit IP address consists of a network address and a host address. The subnet mask determines the number of bits used for the network address and the number of bits used for the host address. The IP address classes have a natural or standard subnet mask, as shown in the table below.

Table 112: IP Address Classes

Class	Address Range	Standard Mask
A	1.0.0.0 to 126.0.0.0	255.0.0.0 or /8
B	128.1.0.0 to 191.254.0.0	255.255.0.0 or /16
C	192.0.1.0 to 223.255.254.0	255.255.255.0 or /24

Reserved addresses include 128.0.0.0, 191.255.0.0, 192.0.0.0, and 223.255.255.0.

When using the standard subnet mask, Class A addresses have one octet for the network, Class B addresses have two octets for the network, and Class C addresses have three octets for the network.

Consider the Class B address 156.26.32.1 with a 24-bit subnet mask, for example. The 24-bit subnet mask selects three octets, 156.26.32, for the network. The last octet is the host address. If the network 156.26.32.1/24 is learned via an IGP and is then redistributed into BGP, if **auto-summary** were enabled, the network would be automatically summarized to the natural mask for a Class B network. The network that BGP would advertise is 156.26.0.0/16. BGP would be advertising that it can reach the entire Class B address space from 156.26.0.0 to 156.26.255.255. If the only network that can be reached via the BGP router is 156.26.32.0/24, BGP would be advertising 254 networks that cannot be reached via this router. This is why the **auto-summary (BGP)** command is disabled by default.

Examples

In the following example, automatic summarization is enabled for IPv4 address family prefixes:

```
Device(config)#router bgp 50000
Device(config-router)#address-family ipv4 unicast
Device(config-router-af)#auto-summary
Device(config-router-af)#network 7.7.7.7 255.255.255.255
```

In the example, there are different subnets, such as 7.7.7.6 and 7.7.7.7 on Loopback interface 6 and Loopback interface 7, respectively. Both **auto-summary** and a **network** command are configured.

```
Device#show ip interface brief
Interface          IP-Address      OK? Method Status          Protocol
Ethernet0/0        100.0.1.7       YES NVRAM up           up
Ethernet0/1        unassigned      YES NVRAM administratively down down
Ethernet0/2        unassigned      YES NVRAM administratively down down
Ethernet0/3        unassigned      YES NVRAM administratively down down
Ethernet1/0        108.7.9.7       YES NVRAM up           up
Ethernet1/1        unassigned      YES NVRAM administratively down down
Ethernet1/2        unassigned      YES NVRAM administratively down down
```

Ethernet1/3	unassigned	YES	NVRAM	administratively	down	down
Loopback6	7.7.7.6	YES	NVRAM	up		up
Loopback7	7.7.7.7	YES	NVRAM	up		up

Note that in the output below, because of the **auto-summary** command, the BGP routing table displays the summarized route 7.0.0.0 instead of 7.7.7.6. The 7.7.7.7/32 network is displayed because it was configured with the **network** command, which is not affected by the **auto-summary** command.

```
Device#show ip bgp
BGP table version is 10, local router ID is 7.7.7.7
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete
      Network          Next Hop            Metric LocPrf Weight Path
*> 6.6.6.6/32      100.0.1.6          0        0 6 i
*> 7.0.0.0          0.0.0.0           0        32768 ?    <-- summarization
*> 7.7.7.7/32      0.0.0.0           0        32768 i    <-- network command
r>i9.9.9.9/32     108.7.9.9          0        100   0 i
*> 100.0.0.0        0.0.0.0           0        32768 ?
r> 100.0.1.0/24    100.0.1.6          0        0 6 ?
*> 108.0.0.0        0.0.0.0           0        32768 ?
r>i108.7.9.0/24   108.7.9.9          0        100   0 ?
*>i200.0.1.0       108.7.9.9          0        0 ?
```

Related Commands	Command	Description
	address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
	address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
	network (BGP and multiprotocol BGP)	Specifies the networks to be advertised by BGP and multiprotocol BGP.

bgp graceful-restart

To enable the Border Gateway Protocol (BGP) graceful restart capability globally for all BGP neighbors, use the **bgp graceful-restart** command in address family or in router configuration mode. To disable the BGP graceful restart capability globally for all BGP neighbors, use the **no** form of this command.

```
bgp graceful-restart [{extended | restart-time seconds | stalepath-time seconds}] [all]
no bgp graceful-restart
```

Syntax Description	extended	(Optional) Enables BGP graceful restart extension.
--------------------	----------	--

bgp graceful-restart

restart-time <i>seconds</i>	(Optional) Sets the maximum time period that the local router will wait for a graceful-restart-capable neighbor to return to normal operation after a restart event occurs. The default value for this argument is 120 seconds. The configurable range of values is from 1 to 3600 seconds.
stalepath-time <i>seconds</i>	(Optional) Sets the maximum time period that the local router will hold stale paths for a restarting peer. All stale paths are deleted after this timer expires. The default value for this argument is 360 seconds. The configurable range of values is from 1 to 3600 seconds.
all	(Optional) Enables BGP graceful restart capability for all address family modes.

Command Default

The following default values are used when this command is entered without any keywords or arguments:

restart-time : 120 seconds **stalepath-time**: 360 seconds



Note Changing the restart and stalepath timer values is not required to enable the BGP graceful restart capability. The default values are optimal for most network deployments, and these values should be adjusted only by an experienced network operator.

Command Modes

Address-family configuration (config-router-af)

Router configuration (config-router)

Command History

Table 113:

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines

The **bgp graceful-restart** command is used to enable or disable the graceful restart capability globally for all BGP neighbors in a BGP network. The graceful restart capability is negotiated between nonstop forwarding (NSF)-capable and NSF-aware peers in OPEN messages during session establishment. If the graceful restart capability is enabled after a BGP session has been established, the session will need to be restarted with a hard reset.

The graceful restart capability is supported by NSF-capable and NSF-aware routers. A router that is NSF-capable can perform a stateful switchover (SSO) operation (graceful restart) and can assist restarting peers by holding routing table information during the SSO operation. A router that is NSF-aware functions like a router that is NSF-capable but cannot perform an SSO operation.

The BGP graceful restart capability is enabled by default when a supporting version of Cisco IOS software is installed. The default timer values for this feature are optimal for most network deployments. We recommend that they are adjusted only by experienced network operators. When adjusting the timer values, the restart timer should not be set to a value greater than the hold time that is carried in the OPEN message. If consecutive restart operations occur, routes (from a restarting router) that were previously marked as stale will be deleted.

**Note**

Changing the restart and stalepath timer values is not required to enable the BGP graceful restart capability. The default values are optimal for most network deployments, and these values should be adjusted only by an experienced network operator.

Examples

In the following example, the BGP graceful restart capability is enabled:

```
Device#configure terminal
Device(config)#router bgp 65000
Device(config-router)#bgp graceful-restart
```

In the following example, the restart timer is set to 130 seconds:

```
Device#configure terminal
Device(config)#router bgp 65000
Device(config-router)#bgp graceful-restart restart-time 130
```

In the following example, the stalepath timer is set to 350 seconds:

```
Device#configure terminal
Device(config)#router bgp 65000
Device(config-router)#bgp graceful-restart stalepath-time 350
```

In the following example, the **extended** keyword is used:

```
Device#configure terminal
Device(config)#router bgp 65000
Device(config-router)#bgp graceful-restart extended
```

Related Commands**Table 114:**

Command	Description
show ip bgp	Displays entries in the BGP routing table.
show ip bgp neighbors	Displays information about the TCP and BGP connections to neighbors.

clear proximity ip bgp

To reset Border Gateway Protocol (BGP) connections using hard or soft reconfiguration, use the **clear proximity ip bgp** command in privileged EXEC mode.

```
clear proximity ip bgp {* | all [autonomous-system-number] neighbor-address | peer-group group-name} [{in [prefix-filter] | out | slow | soft [{in [prefix-filter] | out | slow}]})]
```

Syntax Description

*	Specifies that all current BGP sessions will be reset.
all	(Optional) Specifies the reset of all address family sessions.

clear proximity ip bgp

<i>autonomous-system-number</i>	Number of the autonomous system in which all BGP peer sessions will be reset. Number in the range from 1 to 65535. <ul style="list-style-type: none"> In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXII, Cisco IOS XE Release 2.4, and later releases, 4-byte autonomous system numbers are supported in the range from 65536 to 4294967295 in asplain notation and in the range from 1.0 to 65535.65535 in asdot notation. In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, 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.
<i>neighbor-address</i>	Specifies that only the identified BGP neighbor will be reset. The value for this argument can be an IPv4 or IPv6 address.
peer-group <i>group-name</i>	Specifies that only the identified BGP peer group will be reset.
in	(Optional) Initiates inbound reconfiguration. If neither the in nor out keywords are specified, both inbound and outbound sessions are reset.
prefix-filter	(Optional) Clears the existing outbound route filter (ORF) prefix list to trigger a new route refresh or soft reconfiguration, which updates the ORF prefix list.
out	(Optional) Initiates inbound or outbound reconfiguration. If neither the in nor out keywords are specified, both inbound and outbound sessions are reset.
slow	(Optional) Clears slow-peer status forcefully and moves it to original update group.
soft	(Optional) Initiates a soft reset. Does not tear down the session.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines

The **clear proximity ip bgp** command can be used to initiate a hard reset or soft reconfiguration. A hard reset tears down and rebuilds the specified peering sessions and rebuilds the BGP routing tables. A soft reconfiguration uses stored prefix information to reconfigure and activate BGP routing tables without tearing down existing peering sessions. Soft reconfiguration uses stored update information, at the cost of additional memory for storing the updates, to allow you to apply new BGP policy without disrupting the network. Soft reconfiguration can be configured for inbound or outbound sessions.

Note

Due to the complexity of some of the keywords available for the **clear proximityip bgp** command, some of the keywords are documented as separate commands. All of the complex keywords that are documented separately start with **clear ip bgp**. For example, for information on resetting BGP connections using hard or soft reconfiguration for all BGP neighbors in IPv4 address family sessions, refer to the **clear ip bgp ipv4** command.

Generating Updates from Stored Information

To generate new inbound updates from stored update information (rather than dynamically) without resetting the BGP session, you must preconfigure the local BGP router using the **neighbor soft-reconfiguration inbound** command. This preconfiguration causes the software to store all received updates without modification regardless of whether an update is accepted by the inbound policy. Storing updates is memory intensive and should be avoided if possible.

Outbound BGP soft configuration has no memory overhead and does not require any preconfiguration. You can trigger an outbound reconfiguration on the other side of the BGP session to make the new inbound policy take effect.

Use this command whenever any of the following changes occur:

- Additions or changes to the BGP-related access lists
- Changes to BGP-related weights
- Changes to BGP-related distribution lists
- Changes to BGP-related route maps

Dynamic Inbound Soft Reset

The route refresh capability, as defined in RFC 2918, allows the local router to reset inbound routing tables dynamically by exchanging route refresh requests to supporting peers. The route refresh capability does not store update information locally for non-disruptive policy changes. It instead relies on dynamic exchange with supporting peers. Route refresh is advertised through BGP capability negotiation. All BGP routers must support the route refresh capability.

To determine if a BGP router supports this capability, use the **show ip bgp neighbors** command. The following message is displayed in the output when the router supports the route refresh capability:

```
Received route refresh capability from peer.
```

If all BGP routers support the route refresh capability, use the **clear proximityip bgp** command with the **in** keyword. You need not use the **soft** keyword, because soft reset is automatically assumed when the route refresh capability is supported.

Note

After configuring a soft reset (inbound or outbound), it is normal for the BGP routing process to hold memory. The amount of memory that is held depends on the size of routing tables and the percentage of the memory chunks that are utilized. Partially used memory chunks will be used or released before more memory is allocated from the global router pool.

clear proximity ip bgp

Examples

In the following example, a soft reconfiguration is initiated for the inbound session with the neighbor 10.100.0.1, and the outbound session is unaffected:

```
Device#clear proximity ip bgp 10.100.0.1 soft in
```

In the following example, the route refresh capability is enabled on the BGP neighbor routers and a soft reconfiguration is initiated for the inbound session with the neighbor 172.16.10.2, and the outbound session is unaffected:

```
Device#clear proximity ip bgp 172.16.10.2 in
```

In the following example, a hard reset is initiated for sessions with all routers in the autonomous system numbered 35700:

```
Device#clear proximity ip bgp 35700
```

In the following example, a hard reset is initiated for sessions with all routers in the 4-byte autonomous system numbered 65538 in asplain notation. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXII, Cisco IOS XE Release 2.4, or a later release.

```
Device#clear proximity ip bgp 65538
```

In the following example, a hard reset is initiated for sessions with all routers in the 4-byte autonomous system numbered 1.2 in asdot notation. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(32)S12, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXII, 12.4(24)T, and Cisco IOS XE Release 2.3, or a later release.

```
Device#clear proximity ip bgp 1.2
```

Related Commands

Command	Description
bgp slow-peer split-update-group dynamic permanent	Moves a dynamically detected slow peer to a slow update group.
clear ip bgp ipv4	Resets BGP connections using hard or soft reconfiguration for IPv4 address family sessions.
clear ip bgp ipv6	Resets BGP connections using hard or soft reconfiguration for IPv6 address family sessions.
clear ip bgp vpnv4	Resets BGP connections using hard or soft reconfiguration for VPNv4 address family sessions.
clear ip bgp vpnv6	Resets BGP connections using hard or soft reconfiguration for VPNv6 address family sessions.
neighbor slow-peer split-update-group dynamic permanent	Moves a dynamically detected slow peer to a slow update group.
neighbor soft-reconfiguration	Configures the Cisco IOS software to start storing updates.
router bgp	Configures the BGP routing process.

Command	Description
show ip bgp	Displays entries in the BGP routing table.
show ip bgp neighbors	Displays information about BGP and TCP connections to neighbors.
slow-peer split-update-group dynamic permanent	Moves a dynamically detected slow peer to a slow update group.

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	<table border="1"> <tr> <td>always</td><td>(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.</td></tr> <tr> <td>metric metric-value</td><td>(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.</td></tr> <tr> <td>metric-type type-value</td><td>(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:<ul style="list-style-type: none">• Type 1 external route.• Type 2 external route.The default is type 2 external route.</td></tr> <tr> <td>route-map map-name</td><td>(Optional) The routing process will generate the default route if the route map is satisfied.</td></tr> </table>	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: <ul style="list-style-type: none">• 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.
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: <ul style="list-style-type: none">• Type 1 external route.• Type 2 external route. The default is type 2 external route.								
route-map map-name	(Optional) The routing process will generate the default route if the route map is satisfied.								

Command Default This command is disabled by default. No default external route is generated into the OSPF routing domain.

Command Modes Router configuration (config-router) Router address family topology configuration (config-router-af-topology)

Command History	Cisco IOS XE Everest 16.6.1	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.

default-metric (BGP)

To set a default metric for routes redistributed into Border Gateway Protocol (BGP), use the **default-metric** command in address family or router configuration mode. To remove the configured value and return BGP to default operation, use the **no** form of this command.

default-metric *number*
no default-metric *number*

Syntax Description

<i>number</i>	Default metric value applied to the redistributed route. The range of values for this argument is from 1 to 4294967295.
---------------	---

Command Default

The following is default behavior if this command is not configured or if the **no** form of this command is entered:

- The metric of redistributed interior gateway protocol (IGP) routes is set to a value that is equal to the interior BGP (iBGP) metric.
- The metric of redistributed connected and static routes is set to 0.

When this command is enabled, the metric for redistributed connected routes is set to 0.

Command Modes	Address family configuration (config-router-af) Router configuration (config-router)
----------------------	---

Table 115:

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines	The default-metric command is used to set the metric value for routes redistributed into BGP and can be applied to any external BGP (eBGP) routes received and subsequently advertised internally to iBGP peers. This value is the Multi Exit Discriminator (MED) that is evaluated by BGP during the best path selection process. The MED is a non-transitive value that is processed only within the local autonomous system and adjacent autonomous systems. The default metric is not set if the received route has a MED value.
-------------------------	---



Note When enabled, the **default-metric** command applies a metric value of 0 to redistributed connected routes. The **default-metric** command does not override metric values that are applied with the **redistribute** command.

Examples

In the following example, a metric of 1024 is set for routes redistributed into BGP from OSPF:

```
Device(config)#router bgp 50000
Device(config-router)#address-family ipv4 unicast

Device(config-router-af)#default-metric 1024
Device(config-router-af)#redistribute ospf 10
Device(config-router-af)#end
```

In the following configuration and output examples, a metric of 300 is set for eBGP routes received and advertised internally to an iBGP peer.

```
Device(config)#router bgp 65501
Device(config-router)#no synchronization
Device(config-router)#bgp log-neighbor-changes
Device(config-router)#network 172.16.1.0 mask 255.255.255.0
Device(config-router)#neighbor 172.16.1.1 remote-as 65501
Device(config-router)#neighbor 172.16.1.1 soft-reconfiguration inbound
Device(config-router)#neighbor 192.168.2.2 remote-as 65502
Device(config-router)#neighbor 192.168.2.2 soft-reconfiguration inbound
Device(config-router)#default-metric 300
Device(config-router)#no auto-summary
```

After the above configuration, some routes are received from the eBGP peer at 192.168.2.2 as shown in the output from the **show ip bgp neighbors received-routes** command.

```
Device#show ip bgp neighbors 192.168.2.2 received-routes

BGP table version is 7, local router ID is 192.168.2.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
```

distance (OSPF)

```
Origin codes: i - IGP, e - EGP, ? - incomplete
Network          Next Hop          Metric LocPrf Weight Path
*> 172.17.1.0/24    192.168.2.2           0 65502 i
```

After the received routes from the eBGP peer at 192.168.2.2 are advertised internally to iBGP peers, the output from the **show ip bgp neighbors received-routes** command shows that the metric (MED) has been set to 300 for these routes.

```
Device#show ip bgp neighbors 172.16.1.2 received-routes
BGP table version is 2, local router ID is 172.16.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Network          Next Hop          Metric LocPrf Weight Path
* i172.16.1.0/24    172.16.1.2           0   100     0 i
* i172.17.1.0/24    192.168.2.2         300   100     0 65502 i
Total number of prefixes 2
```

Related Commands	Command	Description
	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	<table border="1"> <tr> <td><i>weight</i></td><td>Administrative distance. Range is 10 to 255. Used alone, the <i>weight</i> argument specifies a default administrative distance that the software uses when no other specification exists for a routing information source. Routes with a distance of 255 are not installed in the routing table. The table in the “Usage Guidelines” section lists the default administrative distances.</td></tr> <tr> <td><i>ip-address</i></td><td>(Optional) IP address in four-part dotted-decimal notation.</td></tr> <tr> <td><i>wildcard-mask</i></td><td>(Optional) Wildcard mask in four-part, dotted-decimal format. A bit set to 1 in the <i>wildcard-mask</i> argument instructs the software to ignore the corresponding bit in the address value.</td></tr> <tr> <td><i>access-list-name</i></td><td>(Optional) Name of an IP access list to be applied to incoming routing updates.</td></tr> </table>	<i>weight</i>	Administrative distance. Range is 10 to 255. Used alone, the <i>weight</i> 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.	<i>ip-address</i>	(Optional) IP address in four-part dotted-decimal notation.	<i>wildcard-mask</i>	(Optional) Wildcard mask in four-part, dotted-decimal format. A bit set to 1 in the <i>wildcard-mask</i> argument instructs the software to ignore the corresponding bit in the address value.	<i>access-list-name</i>	(Optional) Name of an IP access list to be applied to incoming routing updates.
<i>weight</i>	Administrative distance. Range is 10 to 255. Used alone, the <i>weight</i> 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.								
<i>ip-address</i>	(Optional) IP address in four-part dotted-decimal notation.								
<i>wildcard-mask</i>	(Optional) Wildcard mask in four-part, dotted-decimal format. A bit set to 1 in the <i>wildcard-mask</i> argument instructs the software to ignore the corresponding bit in the address value.								
<i>access-list-name</i>	(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 Everest 16.6.1	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 116: 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

eigrp log-neighbor-changes**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.
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 this command.

```
eigrp log-neighbor-changes
no eigrp log-neighbor-changes
```

Syntax Description

This command has no arguments or keywords.

Command Default

Adjacency changes are logged.

Command Modes

Router configuration (config-router) Address-family configuration (config-router-af) Service-family configuration (config-router-sf)

Command History

Release	Modification
Cisco IOS XE Everest 16.6.1	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.

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
```

ip authentication mode eigrp

Syntax Description	<table border="1"> <tr> <td><i>as-number</i></td><td>Autonomous system number to which the authentication applies.</td></tr> <tr> <td><i>key-chain</i></td><td>Name of the authentication key chain.</td></tr> </table>	<i>as-number</i>	Autonomous system number to which the authentication applies.	<i>key-chain</i>	Name of the authentication key chain.
<i>as-number</i>	Autonomous system number to which the authentication applies.				
<i>key-chain</i>	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	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	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	<table border="1"> <tr> <td><i>as-number</i></td><td>Autonomous system number.</td></tr> <tr> <td>md5</td><td>Keyed Message Digest 5 (MD5) authentication.</td></tr> </table>	<i>as-number</i>	Autonomous system number.	md5	Keyed Message Digest 5 (MD5) authentication.
<i>as-number</i>	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 Everest 16.6.1	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:															
<pre>Device(config-if)#ip authentication mode eigrp 10 md5</pre>																
Related Commands	<table border="1"> <thead> <tr> <th>Command</th><th>Description</th></tr> </thead> <tbody> <tr> <td>accept-lifetime</td><td>Sets the time period during which the authentication key on a key chain is received as valid.</td></tr> <tr> <td>ip authentication key-chain eigrp</td><td>Enables authentication of EIGRP packets.</td></tr> <tr> <td>key</td><td>Identifies an authentication key on a key chain.</td></tr> <tr> <td>key chain</td><td>Enables authentication of routing protocols.</td></tr> <tr> <td>key-string (authentication)</td><td>Specifies the authentication string for a key.</td></tr> <tr> <td>send-lifetime</td><td>Sets the time period during which an authentication key on a key chain is valid to be sent.</td></tr> </tbody> </table>		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.
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	<i>as-number</i>	Autonomous system number.
	<i>percent</i>	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)

ip cef load-sharing algorithm

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	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.
	<i>id</i>	(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 Everest 16.6.1	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 community-list

To configure a BGP community list and to control which routes are permitted or denied based on their community values, use the **ip community-list** command in global configuration mode. To delete the community list, use the **no** form of this command.

Standard Community Lists

```
ip community-list {standard | standard list-name} {deny | permit} [community-number] [AA:NN]
[internet] [local-as] [no-advertise] [no-export] [gshut]
no ip community-list {standard | standard list-name}
```

Expanded Community Lists

```
ip community-list {expanded | expanded list-name} {deny | permit} regexp
no ip community-list {expanded | expanded list-name}
```

Syntax Description

standard	Standard community list number from 1 to 99 to identify one or more permit or deny groups of communities.
standard list-name	Configures a named standard community list.
deny	Denies routes that match the specified community or communities.
permit	Permits routes that match the specified community or communities.

ip community-list

<i>community-number</i>	(Optional) 32-bit number from 1 to 4294967200. A single community can be entered or multiple communities can be entered, each separated by a space.
AA :NN	(Optional) Autonomous system number and network number entered in the 4-byte new community format. This value is configured with two 2-byte numbers separated by a colon. A number from 1 to 65535 can be entered for each 2-byte number. A single community can be entered or multiple communities can be entered, each separated by a space.
internet	(Optional) Specifies the Internet community. Routes with this community are advertised to all peers (internal and external).
local-as	(Optional) Specifies the local-as community. Routes with this community are advertised to only peers that are part of the local autonomous system or to only peers within a subautonomous system of a confederation. These routes are not advertised to external peers or to other subautonomous systems within a confederation.
no-advertise	(Optional) Specifies the no-advertise community. Routes with this community are not advertised to any peer (internal or external).

no-export	(Optional) Specifies the no-export community. Routes with this community are advertised to only peers in the same autonomous system or to only other subautonomous systems within a confederation. These routes are not advertised to external peers.
gshut	(Optional) Specifies the Graceful Shutdown (GSHUT) community.
<i>expanded</i>	Expanded community list number from 100 to 500 to identify one or more permit or deny groups of communities.
expanded <i>list-name</i>	Configures a named expanded community list.
<i>regexp</i>	Regular expression that is used to specify a pattern to match against an input string. Note Regular expressions can be used only with expanded community lists.

Command Default BGP community exchange is not enabled by default.

Command Modes Global configuration (config)

Command History *Table 117:*

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines The **ip community-list** command is used to filter BGP routes based on one or more community values. BGP community values are configured as a 32-bit number (old format) or as a 4-byte number (new format). The new community format is enabled when the **ip bgp-community new-format** command is entered in global configuration mode. The new community format consists of a 4-byte value. The first two bytes represent the autonomous system number, and the trailing two bytes represent a user-defined network number. Named and numbered community lists are supported.

ip community-list

BGP community exchange is not enabled by default. The exchange of BGP community attributes between BGP peers is enabled on a per-neighbor basis with the **neighbor send-community** command. The BGP community attribute is defined in RFC 1997 and RFC 1998.

The Internet community is applied to all routes or prefixes by default, until any other community value is configured with this command or the **set community** command.

Use a route map to reference a community list and thereby apply policy routing or set values.

Community List Processing

Once a **permit** value has been configured to match a given set of communities, the community list defaults to an implicit deny for all other community values. Unlike an access list, it is feasible for a community list to contain only **deny** statements.

- When multiple communities are configured in the same **ip community-list** statement, a logical AND condition is created. All community values for a route must match the communities in the community list statement to satisfy an AND condition.
- When multiple communities are configured in separate **ip community-list** statements, a logical OR condition is created. The first list that matches a condition is processed.

Standard Community Lists

Standard community lists are used to configure well-known communities and specific community numbers. A maximum of 16 communities can be configured in a standard community list. If you attempt to configure more than 16 communities, the trailing communities that exceed the limit are not processed or saved to the running configuration file.

Expanded Community Lists

Expanded community lists are used to filter communities using a regular expression. Regular expressions are used to configure patterns to match community attributes. The order for matching using the * or + character is longest construct first. Nested constructs are matched from the outside in. Concatenated constructs are matched beginning at the left side. If a regular expression can match two different parts of an input string, it will match the earliest part first. For more information about configuring regular expressions, see the “Regular Expressions” appendix of the *Terminal Services Configuration Guide*.

Examples

In the following example, a standard community list is configured that permits routes from network 10 in autonomous system 50000:

```
Device(config)#ip community-list 1 permit 50000:10
```

In the following example, a standard community list is configured that permits only routes from peers in the same autonomous system or from subautonomous system peers in the same confederation:

```
Device(config)#ip community-list 1 permit no-export
```

In the following example, a standard community list is configured to deny routes that carry communities from network 40 in autonomous system 65534 and from network 60 in autonomous system 65412. This example shows a logical AND condition; all community values must match in order for the list to be processed.

```
Device(config)#ip community-list 2 deny 65534:40 65412:60
```

In the following example, a named, standard community list is configured that permits all routes within the local autonomous system or permits routes from network 20 in autonomous system 40000. This example shows a logical OR condition; the first match is processed.

```
Device(config)#ip community-list standard RED permit local-as
Device(config)#ip community-list standard RED permit 40000:20
```

In the following example, a standard community list is configured that denies routes with the GSHUT community and permits routes with the local-AS community. This example shows a logical OR condition; the first match is processed.

```
Device(config)#ip community-list 18 deny gshut
Device(config)#ip community-list 18 permit local-as
```

In the following example, an expanded community list is configured that denies routes that carry communities from any private autonomous system:

```
Device(config)#ip community-list 500 deny _64[6-9][0-9][0-9]_I_65[0-9][0-9][0-9]_
```

In the following example, a named expanded community list is configured that denies routes from network 1 to 99 in autonomous system 50000:

```
Device(config)#ip community-list expanded BLUE deny 50000:[0-9][0-9]_
```

Related Commands	Command	Description
	match community	Defines a BGP community that must match the community of a route.
	neighbor send-community	Allows BGP community exchange with a neighbor.
	neighbor shutdown graceful	Configures the BGP Graceful Shutdown feature.
	route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
	set community	Sets the BGP communities attribute.
	set comm-list delete	Removes communities from the community attribute of an inbound or outbound update.
	show ip bgp community	Displays routes that belong to specified BGP communities.
	show ip bgp regexp	Displays routes that match a locally configured regular expression.

ip prefix-list

To create a prefix list or to add a prefix-list entry, use the **ip prefix-list** command in global configuration mode. To delete a prefix-list entry, use the **no** form of this command.

```
ip prefix-list {list-name [seq number] {deny | permit} network/length [ge ge-length] [le le-length]
| description description | sequence-number}
```

no ip prefix-list {list-name [seq number] [{deny | permit} network/length [ge ge-length] [le le-length]] | description description | sequence-number}

Syntax Description	<table border="1"> <tr> <td><i>list-name</i></td><td>Configures a name to identify the prefix list. Do not use the word “detail” or “summary” as a list name because they are keywords in the show ip prefix-list command.</td></tr> <tr> <td>seq</td><td>(Optional) Applies a sequence number to a prefix-list entry.</td></tr> <tr> <td><i>number</i></td><td>(Optional) Integer from 1 to 4294967294. If a sequence number is not entered when configuring this command, default sequence numbering is applied to the prefix list. The number 5 is applied to the first prefix entry, and subsequent unnumbered entries are incremented by 5.</td></tr> <tr> <td>deny</td><td>Denies access for a matching condition.</td></tr> <tr> <td>permit</td><td>Permits access for a matching condition.</td></tr> <tr> <td><i>network / length</i></td><td>Configures the network address and the length of the network mask in bits. The network number can be any valid IP address or prefix. The bit mask can be a number from 1 to 32.</td></tr> <tr> <td>ge</td><td>(Optional) Specifies the lesser value of a range (the “from” portion of the range description) by applying the <i>ge-length</i> argument to the range specified. Note The ge keyword represents the greater than or equal to operator.</td></tr> <tr> <td><i>ge-length</i></td><td>(Optional) Represents the minimum prefix length to be matched.</td></tr> <tr> <td>le</td><td>(Optional) Specifies the greater value of a range (the “to” portion of the range description) by applying the <i>le-length</i> argument to the range specified. Note The le keyword represents the less than or equal to operator.</td></tr> <tr> <td><i>le-length</i></td><td>(Optional) Represents the maximum prefix length to be matched.</td></tr> <tr> <td>description</td><td>(Optional) Configures a descriptive name for the prefix list.</td></tr> <tr> <td><i>description</i></td><td>(Optional) Descriptive name of the prefix list, from 1 to 80 characters in length.</td></tr> <tr> <td>sequence-number</td><td>(Optional) Enables or disables the use of sequence numbers for prefix lists.</td></tr> </table>	<i>list-name</i>	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.	<i>number</i>	(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.	<i>network / length</i>	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 <i>ge-length</i> argument to the range specified. Note The ge keyword represents the greater than or equal to operator.	<i>ge-length</i>	(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 <i>le-length</i> argument to the range specified. Note The le keyword represents the less than or equal to operator.	<i>le-length</i>	(Optional) Represents the maximum prefix length to be matched.	description	(Optional) Configures a descriptive name for the prefix list.	<i>description</i>	(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.
<i>list-name</i>	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.																										
<i>number</i>	(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.																										
<i>network / length</i>	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 <i>ge-length</i> argument to the range specified. Note The ge keyword represents the greater than or equal to operator.																										
<i>ge-length</i>	(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 <i>le-length</i> argument to the range specified. Note The le keyword represents the less than or equal to operator.																										
<i>le-length</i>	(Optional) Represents the maximum prefix length to be matched.																										
description	(Optional) Configures a descriptive name for the prefix list.																										
<i>description</i>	(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 118:*

Release	Modification
Cisco IOS XE Everest 16.6.1	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:

ip hello-interval eigrp

```
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

<i>as-number</i>	Autonomous system number.
<i>seconds</i>	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 Everest 16.6.1	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	<i>as-number</i>	Autonomous system number.
	<i>seconds</i>	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 Everest 16.6.1	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.
------------------	--

ip load-sharing

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-packet | per-destination }
no ip load-sharing per-packet
```

Syntax Description	per-packet	Enables per-packet load balancing for Cisco Express Forwarding on the interface. This functionality and keyword are not supported on all platforms. See "Usage Guidelines" for more information.
	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 Everest 16.6.1	This command was introduced.

Usage Guidelines Per-packet load balancing allows the router to send data packets over successive equal-cost paths without regard to individual destination hosts or user sessions. Path utilization is good, but packets destined for a given destination host might take different paths and might arrive out of order.

Per-destination load balancing allows the device to use multiple, equal-cost paths to achieve load sharing. Packets for a given source-destination host pair are guaranteed to take the same path, even if multiple, equal-cost paths are available. Traffic for different source-destination host pairs tends to take different paths.



Note If you want to enable per-packet load sharing to a particular destination, then all interfaces that can forward traffic to the destination must be enabled for per-packet load sharing.

Examples

The following example shows how to enable per-packet load balancing:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/0/1
Device(config-if)# ip load-sharing per-packet
```

The following example shows how to enable per-destination load balancing:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/0/1
Device(config-if)# ip load-sharing per-destination
```

ip ospf database-filter all out

To filter outgoing link-state advertisements (LSAs) to an Open Shortest Path First (OSPF) interface, use the **ip ospf database-filter all out** command in interface or virtual network interface configuration modes. To restore the forwarding of LSAs to the interface, use the **no** form of this command.

```
ip ospf database-filter all out [disable]
no ip ospf database-filter all out
```

Syntax Description	<table border="1"> <tr> <td>disable</td><td>(Optional) Disables the filtering of outgoing LSAs to an OSPF interface; all outgoing LSAs are flooded to the interface.</td></tr> <tr> <td>Note</td><td>This keyword is available only in virtual network interface mode.</td></tr> </table>	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.
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 Everest 16.6.1	This command was introduced.

Usage Guidelines This command performs the same function that the **neighbor database-filter** command performs on a neighbor basis.

ip ospf name-lookup

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 Everest 16.6.1	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	<i>as-number</i>	Autonomous system number.						
Command Default	The behavior of this command is enabled by default.							
Command Modes	Interface configuration (config-if) Virtual network interface (config-if-vnet)							
Command History	<table border="1"> <tr> <th>Release</th> <th>Modification</th> </tr> <tr> <td>Cisco IOS XE Everest 16.6.1</td> <td>This command was introduced.</td> </tr> </table>		Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.		
Release	Modification							
Cisco IOS XE Everest 16.6.1	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:							
<pre>Device(config-if)#ip split-horizon eigrp 101</pre>								
Related Commands	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>ip split-horizon (RIP)</td> <td>Enables the split horizon mechanism.</td> </tr> <tr> <td>neighbor (EIGRP)</td> <td>Defines a neighboring router with which to exchange routing information.</td> </tr> </tbody> </table>		Command	Description	ip split-horizon (RIP)	Enables the split horizon mechanism.	neighbor (EIGRP)	Defines a neighboring router with which to exchange routing information.
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	<i>as-number</i>	Autonomous system number.
	<i>ip-address</i>	Summary IP address to apply to an interface.
	<i>mask</i>	Subnet mask.
	<i>admin-distance</i>	(Optional) Administrative distance. Range: 0 to 255. Note Starting with Cisco IOS XE Release 3.2S, the <i>admin-distance</i> argument was removed. Use the summary-metric command to configure the administrative distance.

ip summary-address eigrp

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 Everest 16.6.1	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.

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.
--------------------	-----	--

metric weights (EIGRP)

<i>k1 k2 k3 k4 k5 k6</i>	(Optional) Constants that convert an EIGRP metric vector into a scalar quantity. Valid values are 0 to 255. Given below are the default values: <ul style="list-style-type: none">• <i>k1</i>: 1• <i>k2</i>: 0• <i>k3</i>: 1• <i>k4</i>: 0• <i>k5</i>: 0• <i>k6</i>: 0 <p>Note In address family configuration mode, if the values are not specified, default values are configured. The <i>k6</i> argument is supported only in address family configuration mode.</p>
--------------------------	---

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 Everest 16.6.1	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= $10^7/\text{minimum interface bandwidth (in kilobits per second)} * 256$

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 FFFFFFFFFF (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 advertisement-interval

To set the minimum route advertisement interval (MRAI) between the sending of BGP routing updates, use the **neighbor advertisement-interval** command in address family or router configuration mode. To restore the default value, use the **no** form of this command.

```
neighbor {ip-address|peer-group-name} advertisement-interval seconds
no neighbor {ip-address|peer-group-name} advertisement-interval seconds
```

Syntax Description	<i>ip-address</i>	IP address of the neighbor.
	<i>peer-group-name</i>	Name of a BGP peer group.
	<i>seconds</i>	Time (in seconds) is specified by an integer ranging from 0 to 600.

Command Default eBGP sessions not in a VRF: 30 seconds

eBGP sessions in a VRF: 0 seconds

iBGP sessions: 0 seconds

Command Modes Router configuration (config-router)

neighbor default-originate**Command History****Table 119:**

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines

When the MRAI is equal to 0 seconds, BGP routing updates are sent as soon as the BGP routing table changes. If you specify a BGP peer group by using the *peer-group-name* argument, all the members of the peer group will inherit the characteristic configured with this command.

Examples

The following router configuration mode example sets the minimum time between sending BGP routing updates to 10 seconds:

```
router bgp 5
  neighbor 10.4.4.4 advertisement-interval 10
```

The following address family configuration mode example sets the minimum time between sending BGP routing updates to 10 seconds:

```
router bgp 5
  address-family ipv4 unicast
    neighbor 10.4.4.4 advertisement-interval 10
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
neighbor peer-group (creating)	Creates a BGP peer group.

neighbor default-originate

To allow a BGP speaker (the local router) to send the default route 0.0.0.0 to a neighbor for use as a default route, use the **neighbor default-originate** command in address family or router configuration mode. To send no route as a default, use the **no** form of this command.

```
neighbor {ip-address|peer-group-name} default-originate [route-map map-name]
no neighbor {ip-address|peer-group-name} default-originate [route-map map-name]
```

Syntax Description

<i>ip-address</i>	IP address of the neighbor.
<i>peer-group-name</i>	Name of a BGP peer group.

route-map <i>map-name</i>	(Optional) Name of the route map. The route map allows route 0.0.0.0 to be injected conditionally.
----------------------------------	--

Command Default No default route is sent to the neighbor.

Command Modes Address family configuration (config-router-af)
Router configuration (config-router)

Table 120:

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines This command does not require the presence of 0.0.0.0 in the local router. When used with a route map, the default route 0.0.0.0 is injected if the route map contains a **match ip address** clause and there is a route that matches the IP access list exactly. The route map can contain other match clauses also.

You can use standard or extended access lists with the **neighbor default-originate** command.

Examples In the following router configuration example, the local router injects route 0.0.0.0 to the neighbor 172.16.2.3 unconditionally:

```
router bgp 109
network 172.16.0.0
neighbor 172.16.2.3 remote-as 200
neighbor 172.16.2.3 default-originate
```

In the following example, the local router injects route 0.0.0.0 to the neighbor 172.16.2.3 only if there is a route to 192.168.68.0 (that is, if a route with any mask exists, such as 255.255.255.0 or 255.255.0.0):

```
router bgp 109
network 172.16.0.0
neighbor 172.16.2.3 remote-as 200
neighbor 172.16.2.3 default-originate route-map default-map
!
route-map default-map 10 permit
  match ip address 1
!
access-list 1 permit 192.168.68.0
```

In the following example, the last line of the configuration has been changed to show the use of an extended access list. The local router injects route 0.0.0.0 to the neighbor 172.16.2.3 only if there is a route to 192.168.68.0 with a mask of 255.255.0.0:

```
router bgp 109
network 172.16.0.0
neighbor 172.16.2.3 remote-as 200
neighbor 172.16.2.3 default-originate route-map default-map
!
route-map default-map 10 permit
  match ip address 100
```

neighbor description

```

!
access-list 100 permit ip host 192.168.68.0 host 255.255.0.0

```

Related Commands	Command	Description
	address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
	address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
	neighbor ebgp-multihop	Accepts and attempts BGP connections to external peers residing on networks that are not directly connected.

neighbor description

To associate a description with a neighbor, use the **neighbor description** command in router configuration mode or address family configuration mode. To remove the description, use the **no** form of this command.

```

neighbor {ip-address|peer-group-name} description text
no neighbor {ip-address|peer-group-name} description [text]

```

Syntax Description	<i>ip-address</i>	IP address of the neighbor.
	<i>peer-group-name</i>	Name of an EIGRP peer group. This argument is not available in address-family configuration mode.
	<i>text</i>	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 Everest 16.6.1	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.

neighbor ebgp-multihop

To accept and attempt BGP connections to external peers residing on networks that are not directly connected, use the **neighbor ebgp-multihop** command in router configuration mode. To return to the default, use the **no** form of this command.

```

neighbor {ip-address|ipv6-address|peer-group-name} ebgp-multihop [ttl]
no neighbor {ip-address|ipv6-address|peer-group-name} ebgp-multihop

```

Syntax Description	<table border="1"> <tr> <td><i>ip-address</i></td><td>IP address of the BGP-speaking neighbor.</td></tr> <tr> <td><i>ipv6-address</i></td><td>IPv6 address of the BGP-speaking neighbor.</td></tr> <tr> <td><i>peer-group-name</i></td><td>Name of a BGP peer group.</td></tr> <tr> <td><i>ttl</i></td><td>(Optional) Time-to-live in the range from 1 to 255 hops.</td></tr> </table>	<i>ip-address</i>	IP address of the BGP-speaking neighbor.	<i>ipv6-address</i>	IPv6 address of the BGP-speaking neighbor.	<i>peer-group-name</i>	Name of a BGP peer group.	<i>ttl</i>	(Optional) Time-to-live in the range from 1 to 255 hops.
<i>ip-address</i>	IP address of the BGP-speaking neighbor.								
<i>ipv6-address</i>	IPv6 address of the BGP-speaking neighbor.								
<i>peer-group-name</i>	Name of a BGP peer group.								
<i>ttl</i>	(Optional) Time-to-live in the range from 1 to 255 hops.								

Command Default Only directly connected neighbors are allowed.

Command Modes Router configuration (config-router)

Table 121:

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines This feature should be used only under the guidance of Cisco technical support staff.

If you specify a BGP peer group by using the *peer-group-name* argument, all the members of the peer group will inherit the characteristic configured with this command.

To prevent the creation of loops through oscillating routes, the multihop will not be established if the only route to the multihop peer is the default route (0.0.0.0).

neighbor maximum-prefix (BGP)**Examples**

The following example allows connections to or from neighbor 10.108.1.1, which resides on a network that is not directly connected:

```
Device(config)#router bgp 109
Device(config-router)#neighbor 10.108.1.1 ebgp-multihop
```

Related Commands	Command	Description
	neighbor advertise-map non-exist-map	Allows a BGP speaker (the local router) to send the default route 0.0.0.0 to a neighbor for use as a default route.
	neighbor peer-group (creating)	Creates a BGP peer group.
	network (BGP and multiprotocol BGP)	Specifies the list of networks for the BGP routing process.

neighbor maximum-prefix (BGP)

To control how many prefixes can be received from a neighbor, use the **neighbor maximum-prefix** command in router configuration mode. To disable this function, use the **no** form of this command.

```
neighbor {ip-address|peer-group-name} maximum-prefix maximum [threshold] [restart restart-interval]
[warning-only]
no neighbor {ip-address|peer-group-name} maximum-prefix maximum
```

Syntax Description	ip-address	IP address of the neighbor.
	peer-group-name	Name of a Border Gateway Protocol (BGP) peer group.
	maximum	Maximum number of prefixes allowed from the specified neighbor. The number of prefixes that can be configured is limited only by the available system resources on a router.
	threshold	(Optional) Integer specifying at what percentage of the <i>maximum-prefix</i> limit the router starts to generate a warning message. The range is from 1 to 100; the default is 75.
	restart	(Optional) Configures the router that is running BGP to automatically reestablish a peering session that has been disabled because the <i>maximum-prefix</i> limit has been exceeded. The restart timer is configured with the <i>restart-interval</i> argument.
	restart-interval	(Optional) Time interval (in minutes) that a peering session is reestablished. The range is from 1 to 65535 minutes.
	warning-only	(optional) Allows the router to generate a sys-log message when the <i>maximum-prefix</i> limit is exceeded, instead of terminating the peering session.

Command Default

This command is disabled by default. Peering sessions are disabled when the maximum number of prefixes is exceeded. If the *restart-interval* argument is not configured, a disabled session will stay down after the *maximum-prefix* limit is exceeded.

threshold : 75 percent

Command Modes

Router configuration (config-router)

Command History**Table 122:**

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines

The **neighbor maximum-prefix** command allows you to configure a maximum number of prefixes that a Border Gateway Protocol (BGP) routing process will accept from the specified peer. This feature provides a mechanism (in addition to distribute lists, filter lists, and route maps) to control prefixes received from a peer.

When the number of received prefixes exceeds the maximum number configured, BGP disables the peering session (by default). If the **restart** keyword is configured, BGP will automatically reestablish the peering session at the configured time interval. If the **restart** keyword is not configured and a peering session is terminated because the maximum prefix limit has been exceeded, the peering session will not be reestablished until the **clear ip bgp** command is entered. If the **warning-only** keyword is configured, BGP sends only a log message and continues to peer with the sender.

There is no default limit on the number of prefixes that can be configured with this command. Limitations on the number of prefixes that can be configured are determined by the amount of available system resources.

Examples

In the following example, the maximum prefixes that will be accepted from the 192.168.1.1 neighbor is set to 1000:

```
Device(config)#router bgp 40000
Device(config-router)#network 192.168.0.0
Device(config-router)#neighbor 192.168.1.1 maximum-prefix 1000
```

In the following example, the maximum number of prefixes that will be accepted from the 192.168.2.2 neighbor is set to 5000. The router is also configured to display warning messages when 50 percent of the maximum-prefix limit (2500 prefixes) has been reached.

```
Device(config)#router bgp 40000
Device(config-router)#network 192.168.0.0
Device(config-router)#neighbor 192.168.2.2 maximum-prefix 5000 50
```

In the following example, the maximum number of prefixes that will be accepted from the 192.168.3.3 neighbor is set to 2000. The router is also configured to reestablish a disabled peering session after 30 minutes.

```
Device(config)#router bgp 40000
Device(config-router) network 192.168.0.0
Device(config-router)#neighbor 192.168.3.3 maximum-prefix 2000 restart 30
```

In the following example, warning messages will be displayed when the threshold of the maximum-prefix limit ($500 \times 0.75 = 375$) for the 192.168.4.4 neighbor is exceeded:

```
Device(config)#router bgp 40000
```

neighbor peer-group (assigning members)

```
Device(config-router)#network 192.168.0.0
Device(config-router)#neighbor 192.168.4.4 maximum-prefix 500 warning-only
```

Related Commands

Command	Description
clear ip bgp	Resets a BGP connection using BGP soft reconfiguration.

neighbor peer-group (assigning members)

To configure a BGP neighbor to be a member of a peer group, use the **neighbor peer-group** command in address family or router configuration mode. To remove the neighbor from the peer group, use the **no** form of this command.

```
neighbor {ip-address|ipv6-address} peer-group peer-group-name
no neighbor {ip-address|ipv6-address} peer-group peer-group-name
```

Syntax Description

<i>ip-address</i>	IP address of the BGP neighbor that belongs to the peer group specified by the <i>peer-group-name</i> argument.
<i>ipv6-address</i>	IPv6 address of the BGP neighbor that belongs to the peer group specified by the <i>peer-group-name</i> argument.
<i>peer-group-name</i>	Name of the BGP peer group to which this neighbor belongs.

Command Default

There are no BGP neighbors in a peer group.

Command Modes

Address family configuration (config-router-af)
Router configuration (config-router)

Command History

Table 123:

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines

The neighbor at the IP address indicated inherits all the configured options of the peer group.

Note

Using the **no** form of the **neighbor peer-group** command removes all of the BGP configuration for that neighbor, not just the peer group association.

Examples

The following router configuration mode example assigns three neighbors to the peer group named internal:

```

Device(config)#router bgp 100
Device(config-router)#neighbor internal peer-group
Device(config-router)#neighbor internal remote-as 100
Device(config-router)#neighbor internal update-source loopback 0
Device(config-router)#neighbor internal route-map set-med out
Device(config-router)#neighbor internal filter-list 1 out
Device(config-router)#neighbor internal filter-list 2 in
Device(config-router)#neighbor 172.16.232.53 peer-group internal
Device(config-router)#neighbor 172.16.232.54 peer-group internal
Device(config-router)#neighbor 172.16.232.55 peer-group internal
Device(config-router)#neighbor 172.16.232.55 filter-list 3 in

```

The following address family configuration mode example assigns three neighbors to the peer group named internal:

```

Device(config)#router bgp 100
Device(config-router)#address-family ipv4 unicast
Device(config-router)#neighbor internal peer-group
Device(config-router)#neighbor internal remote-as 100
Device(config-router)#neighbor internal update-source loopback 0
Device(config-router)#neighbor internal route-map set-med out
Device(config-router)#neighbor internal filter-list 1 out
Device(config-router)#neighbor internal filter-list 2 in
Device(config-router)#neighbor 172.16.232.53 peer-group internal
Device(config-router)#neighbor 172.16.232.54 peer-group internal
Device(config-router)#neighbor 172.16.232.55 peer-group internal
Device(config-router)#neighbor 172.16.232.55 filter-list 3 in

```

Related Commands	Command	Description
	address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
	address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
	neighbor peer-group (creating)	Creates a BGP peer group.
	neighbor shutdown	Disables a neighbor or peer group.

neighbor peer-group (creating)

To create a BGP or multiprotocol BGP peer group, use the **neighbor peer-group** command in address family or router configuration mode. To remove the peer group and all of its members, use the **no** form of this command.

```

neighbor peer-group-name peer-group
no neighbor peer-group-name peer-group

```

Syntax Description	<i>peer-group-name</i>	Name of the BGP peer group.
--------------------	------------------------	-----------------------------

neighbor peer-group (creating)

Command Default There is no BGP peer group.

Command Modes Address family configuration (config-router-af)
Router configuration (config-router)

Table 124:

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines Often in a BGP or multiprotocol BGP speaker, many neighbors are configured with the same update policies (that is, same outbound route maps, distribute lists, filter lists, update source, and so on). Neighbors with the same update policies can be grouped into peer groups to simplify configuration and make update calculation more efficient.



Note Peer group members can span multiple logical IP subnets, and can transmit, or pass along, routes from one peer group member to another.

Once a peer group is created with the **neighbor peer-group** command, it can be configured with the **neighbor** commands. By default, members of the peer group inherit all the configuration options of the peer group. Members also can be configured to override the options that do not affect outbound updates.

All the peer group members will inherit the current configuration as well as changes made to the peer group. Peer group members will always inherit the following configuration options by default:

- remote-as (if configured)
- version
- update-source
- outbound route-maps
- outbound filter-lists
- outbound distribute-lists
- minimum-advertisement-interval
- next-hop-self

If a peer group is not configured with a remote-as option, the members can be configured with the **neighbor {ip-address | peer-group-name} remote-as** command. This command allows you to create peer groups containing external BGP (eBGP) neighbors.

Examples

The following example configurations show how to create these types of neighbor peer group:

- internal Border Gateway Protocol (iBGP) peer group
- eBGP peer group
- Multiprotocol BGP peer group

In the following example, the peer group named internal configures the members of the peer group to be iBGP neighbors. By definition, this is an iBGP peer group because the **router bgp** command and the **neighbor remote-as** command indicate the same autonomous system (in this case, autonomous system 100). All the peer group members use loopback 0 as the update source and use set-med as the outbound route map. The **neighbor internal filter-list 2 in** command shows that, except for 172.16.232.55, all the neighbors have filter list 2 as the inbound filter list.

```
router bgp 100
neighbor internal peer-group
neighbor internal remote-as 100
neighbor internal update-source loopback 0
neighbor internal route-map set-med out
neighbor internal filter-list 1 out
neighbor internal filter-list 2 in
neighbor 172.16.232.53 peer-group internal
neighbor 172.16.232.54 peer-group internal
neighbor 172.16.232.55 peer-group internal
neighbor 172.16.232.55 filter-list 3 in
```

The following example defines the peer group named external-peers without the **neighbor remote-as** command. By definition, this is an eBGP peer group because each individual member of the peer group is configured with its respective autonomous system number separately. Thus the peer group consists of members from autonomous systems 200, 300, and 400. All the peer group members have the set-metric route map as an outbound route map and filter list 99 as an outbound filter list. Except for neighbor 172.16.232.110, all of them have 101 as the inbound filter list.

```
router bgp 100
neighbor external-peers peer-group
neighbor external-peers route-map set-metric out
neighbor external-peers filter-list 99 out
neighbor external-peers filter-list 101 in
neighbor 172.16.232.90 remote-as 200
neighbor 172.16.232.90 peer-group external-peers
neighbor 172.16.232.100 remote-as 300
neighbor 172.16.232.100 peer-group external-peers
neighbor 172.16.232.110 remote-as 400
neighbor 172.16.232.110 peer-group external-peers
neighbor 172.16.232.110 filter-list 400 in
```

In the following example, all members of the peer group are multicast-capable:

```
router bgp 100
neighbor 10.1.1.1 remote-as 1
neighbor 172.16.2.2 remote-as 2
address-family ipv4 multicast
neighbor mygroup peer-group
neighbor 10.1.1.1 peer-group mygroup
neighbor 172.16.2.2 peer-group mygroup
neighbor 10.1.1.1 activate
neighbor 172.16.2.2 activate
```

neighbor route-map

Related Commands	Command	Description
	address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
	address-family vpng4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPGv4 address prefixes.
	clear ip bgp peer-group	Removes all the members of a BGP peer group.
	show ip bgp peer-group	Displays information about BGP peer groups.

neighbor route-map

To apply a route map to incoming or outgoing routes, use the **neighbor route-map** command in address family or router configuration mode. To remove a route map, use the **no** form of this command.

```
neighbor{ip-address|peer-group-name | ipv6-address[%]} route-map map-name {in | out}
no neighbor{ip-address|peer-group-name | ipv6-address[%]} route-map map-name {in | out}
```

Syntax Description	<i>ip-address</i>	IP address of the neighbor.
	<i>peer-group-name</i>	Name of a BGP or multiprotocol BGP peer group.
	<i>ipv6-address</i>	IPv6 address of the neighbor.
	<i>%</i>	(Optional) IPv6 link-local address identifier. This keyword needs to be added whenever a link-local IPv6 address is used outside the context of its interface.
	<i>map-name</i>	Name of a route map.
	in	Applies route map to incoming routes.
	out	Applies route map to outgoing routes.

Command Default No route maps are applied to a peer.

Command Modes Router configuration (config-router)

Table 125:

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines When specified in address family configuration mode, this command applies a route map to that particular address family only. When specified in router configuration mode, this command applies a route map to IPv4 or IPv6 unicast routes only.

If an outbound route map is specified, it is proper behavior to only advertise routes that match at least one section of the route map.

If you specify a BGP or multiprotocol BGP peer group by using the *peer-group-name* argument, all the members of the peer group will inherit the characteristic configured with this command. Specifying the command for a neighbor overrides the inbound policy that is inherited from the peer group.

The % keyword is used whenever link-local IPv6 addresses are used outside the context of their interfaces. This keyword does not need to be used for non-link-local IPv6 addresses.

Examples

The following router configuration mode example applies a route map named internal-map to a BGP incoming route from 172.16.70.24:

```
router bgp 5
neighbor 172.16.70.24 route-map internal-map in
route-map internal-map
match as-path 1
set local-preference 100
```

The following address family configuration mode example applies a route map named internal-map to a multiprotocol BGP incoming route from 172.16.70.24:

```
router bgp 5
address-family ipv4 multicast
neighbor 172.16.70.24 route-map internal-map in
route-map internal-map
match as-path 1
set local-preference 100
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IP Version 4 address prefixes.
address-family ipv6	Enters address family configuration mode for configuring routing sessions such as BGP that use standard IPv6 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPN Version 4 address prefixes.
address-family vpnv6	Places the router in address family configuration mode for configuring routing sessions that use standard VPNv6 address prefixes.
neighbor remote-as	Creates a BGP peer group.

neighbor update-source

To have the Cisco software allow Border Gateway Protocol (BGP) sessions to use any operational interface for TCP connections, use the **neighbor update-source** command in router configuration mode. To restore

neighbor update-source

the interface assignment to the closest interface, which is called the best local address, use the **no** form of this command.

neighbor{ip-address | ipv6-address[%]peer-group-name}update-source interface-type interface-number
neighbor{ip-address | ipv6-address[%]peer-group-name}update-source interface-type interface-number

Syntax Description	<table border="1"> <tr> <td><i>ip-address</i></td><td>IPv4 address of the BGP-speaking neighbor.</td></tr> <tr> <td><i>ipv6-address</i></td><td>IPv6 address of the BGP-speaking neighbor.</td></tr> <tr> <td><i>%</i></td><td>(Optional) IPv6 link-local address identifier. This keyword needs to be added whenever a link-local IPv6 address is used outside the context of its interface.</td></tr> <tr> <td><i>peer-group-name</i></td><td>Name of a BGP peer group.</td></tr> <tr> <td><i>interface-type</i></td><td>Interface type.</td></tr> <tr> <td><i>interface-number</i></td><td>Interface number.</td></tr> </table>	<i>ip-address</i>	IPv4 address of the BGP-speaking neighbor.	<i>ipv6-address</i>	IPv6 address of the BGP-speaking neighbor.	<i>%</i>	(Optional) IPv6 link-local address identifier. This keyword needs to be added whenever a link-local IPv6 address is used outside the context of its interface.	<i>peer-group-name</i>	Name of a BGP peer group.	<i>interface-type</i>	Interface type.	<i>interface-number</i>	Interface number.
<i>ip-address</i>	IPv4 address of the BGP-speaking neighbor.												
<i>ipv6-address</i>	IPv6 address of the BGP-speaking neighbor.												
<i>%</i>	(Optional) IPv6 link-local address identifier. This keyword needs to be added whenever a link-local IPv6 address is used outside the context of its interface.												
<i>peer-group-name</i>	Name of a BGP peer group.												
<i>interface-type</i>	Interface type.												
<i>interface-number</i>	Interface number.												

Command Default Best local address

Command Modes Router configuration (config-router)

Command History *Table 126:*

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines This command can work in conjunction with the loopback interface feature described in the “Interface Configuration Overview” chapter of the Cisco IOS Interface and Hardware Component Configuration Guide.

If you specify a BGP peer group by using the *peer-group-name* argument, all the members of the peer group will inherit the characteristic configured with this command.

The **neighbor update-source** command must be used to enable IPv6 link-local peering for internal or external BGP sessions.

The *%* keyword is used whenever link-local IPv6 addresses are used outside the context of their interfaces and for these link-local IPv6 addresses you must specify the interface they are on. The syntax becomes <IPv6 local-link address>%<interface name>, for example, FE80::1%Ethernet1/0. Note that the interface type and number must not contain any spaces, and be used in full-length form because name shortening is not supported in this situation. The *%* keyword and subsequent interface syntax is not used for non-link-local IPv6 addresses.

Examples

The following example sources BGP TCP connections for the specified neighbor with the IP address of the loopback interface rather than the best local address:

```
Device(config)#router bgp 65000
Device(config-router)#network 172.16.0.0
Device(config-router)#neighbor 172.16.2.3 remote-as 110
Device(config-router)#neighbor 172.16.2.3 update-source Loopback0
```

The following example sources IPv6 BGP TCP connections for the specified neighbor in autonomous system 65000 with the global IPv6 address of loopback interface 0 and the specified neighbor in autonomous system 65400 with the link-local IPv6 address of Fast Ethernet interface 0/0. Note that the link-local IPv6 address of FE80::2 is on Ethernet interface 1/0.

```
Device(config)#router bgp 65000
Device(config-router)#neighbor 3ffe::3 remote-as 65000
Device(config-router)#neighbor 3ffe::3 update-source Loopback0
Device(config-router)#neighbor fe80::2%Ethernet1/0 remote-as 65400
Device(config-router)#neighbor fe80::2%Ethernet1/0 update-source FastEthernet 0/0
Device(config-router)#address-family ipv6
Device(config-router)#neighbor 3ffe::3 activate
Device(config-router)#neighbor fe80::2%Ethernet1/0 activate
Device(config-router)#exit-address-family
```

Related Commands	Command	Description
	neighbor activate	Enables the exchange of information with a BGP neighboring router.
	neighbor remote-as	Adds an entry to the BGP or multiprotocol BGP neighbor table.

network (BGP and multiprotocol BGP)

To specify the networks to be advertised by the Border Gateway Protocol (BGP) and multiprotocol BGP routing processes, use the **network** command in address family or router configuration mode. To remove an entry from the routing table, use the **no** form of this command.

```
network {network-number [mask network-mask]nsap-prefix} [route-map map-tag]
no network {network-number [mask network-mask]nsap-prefix} [route-map map-tag]
```

Syntax Description	<table border="1"> <tr> <td><i>network-number</i></td><td>Network that BGP or multiprotocol BGP will advertise.</td></tr> <tr> <td>mask <i>network-mask</i></td><td>(Optional) Network or subnetwork mask with mask address.</td></tr> <tr> <td>nsap-prefix</td><td>Network service access point (NSAP) prefix of the Connectionless Network Service (CLNS) network that BGP or multiprotocol BGP will advertise. This argument is used only under NSAP address family configuration mode.</td></tr> <tr> <td>route-map <i>map-tag</i></td><td>(Optional) Identifier of a configured route map. The route map should be examined to filter the networks to be advertised. If not specified, all networks are advertised. If the keyword is specified, but no route map tags are listed, no networks will be advertised.</td></tr> </table>	<i>network-number</i>	Network that BGP or multiprotocol BGP will advertise.	mask <i>network-mask</i>	(Optional) Network or subnetwork mask with mask address.	nsap-prefix	Network service access point (NSAP) prefix of the Connectionless Network Service (CLNS) network that BGP or multiprotocol BGP will advertise. This argument is used only under NSAP address family configuration mode.	route-map <i>map-tag</i>	(Optional) Identifier of a configured route map. The route map should be examined to filter the networks to be advertised. If not specified, all networks are advertised. If the keyword is specified, but no route map tags are listed, no networks will be advertised.
<i>network-number</i>	Network that BGP or multiprotocol BGP will advertise.								
mask <i>network-mask</i>	(Optional) Network or subnetwork mask with mask address.								
nsap-prefix	Network service access point (NSAP) prefix of the Connectionless Network Service (CLNS) network that BGP or multiprotocol BGP will advertise. This argument is used only under NSAP address family configuration mode.								
route-map <i>map-tag</i>	(Optional) Identifier of a configured route map. The route map should be examined to filter the networks to be advertised. If not specified, all networks are advertised. If the keyword is specified, but no route map tags are listed, no networks will be advertised.								

Command Default No networks are specified.

Command Modes Address family configuration (config-router-af)
Router configuration (config-router)

network (BGP and multiprotocol BGP)**Command History****Table 127:**

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines

BGP and multiprotocol BGP networks can be learned from connected routes, from dynamic routing, and from static route sources.

The maximum number of **network** commands you can use is determined by the resources of the router, such as the configured NVRAM or RAM.

Examples

The following example sets up network 10.108.0.0 to be included in the BGP updates:

```
Device(config)#router bgp 65100
Device(config-router)#network 10.108.0.0
```

The following example sets up network 10.108.0.0 to be included in the multiprotocol BGP updates:

```
Device(config)#router bgp 64800
Device(config-router)#address family ipv4 multicast
Device(config-router)#network 10.108.0.0
```

The following example advertises NSAP prefix 49.6001 in the multiprotocol BGP updates:

```
Device(config)#router bgp 64500
Device(config-router)#address-family nsap
Device(config-router)#network 49.6001
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Enters the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IP Version 4 address prefixes.
address-family vpnv4	Enters the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
default-information originate (BGP)	Allows the redistribution of network 0.0.0.0 into BGP.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another.
router bgp	Configures the BGP routing 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	<i>ip-address</i>	IP address of the directly connected network.
	<i>wildcard-mask</i>	(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 Everest 16.6.1	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
```

nsf (EIGRP)

```
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 Everest 16.6.1	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.
	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-number} {in | out} offset [interface-type interface-number]
no offset-list {access-list-number} {in | out} offset [interface-type interface-number]
```

Syntax Description	<i>access-list-number</i> <i>access-list-name</i>	Standard access list number or name to be applied. Access list number 0 indicates all networks (networks, prefixes, or routes). If the <i>offset</i> value is 0, no action is taken.
	in	Applies the access list to incoming metrics.
	out	Applies the access list to outgoing metrics.
	<i>offset</i>	Positive offset to be applied to metrics for networks matching the access list. If the offset is 0, no action is taken.
	<i>interface-type</i>	(Optional) Interface type to which the offset list is applied.
	<i>interface-number</i>	(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.

redistribute (IP)

Command Modes Router configuration (config-router) Address family topology configuration (config-router-af-topology)

Table 128:

Release	Modification
Cisco IOS XE Everest 16.6.1	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		
	<i>protocol</i>	<p>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].</p> <p>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.</p> <p>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).</p> <p>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.</p>
	<i>process-id</i>	<p>(Optional) For the application keyword, this is the name of an application.</p> <p>For the bgp or eigrp keyword, this is an autonomous system number, which is a 16-bit decimal number.</p> <p>For the isis keyword, this is an optional <i>tag</i> 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.</p> <p>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.</p> <p>For the rip keyword, no <i>process-id</i> value is needed.</p> <p>For the application keyword, this is the name of an application.</p> <p>By default, no process ID is defined.</p>
	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.

<i>autonomous-system-number</i>	(Optional) Autonomous system number for the redistributed route. The range is from 1 to 65535. <ul style="list-style-type: none"> • 4-byte autonomous system numbers are supported in the range from 1.0 to 65535.65535 in asdot notation only. <p>For more details about autonomous system number formats, see the router bgp command.</p>
metric <i>metric-value</i>	(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 <i>type value</i>	(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: <ul style="list-style-type: none"> • 1—Type 1 external route • 2—Type 2 external route <p>If a metric-type is not specified, the Cisco IOS software adopts a Type 2 external route.</p> <p>For IS-IS, it can be one of two values:</p> <ul style="list-style-type: none"> • internal—IS-IS metric that is < 63. • external—IS-IS metric that is > 64 < 128. <p>The default is internal.</p>
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: <ul style="list-style-type: none"> • 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. <p>The default is internal.</p>

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.
<i>map-tag</i>	(Optional) Identifier of a configured route map.
subnets	(Optional) For redistributing routes into OSPF, the scope of redistribution for the specified protocol. By default, no subnets are defined.
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 Everest 16.6.1	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.)

When routes are redistributed into OSPF, only routes that are not subnetted are redistributed if the **subnets** keyword is not specified.



Note Depending on your release the **subnets** keyword is automatically appended when you use the **redistribute ospf** command. This automatic addition results in the redistribution of classless OSPF routes.

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):

redistribute (IP)

```

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.

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	<i>ip-address</i>	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 Everest 16.6.1	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 bgp

To configure the Border Gateway Protocol (BGP) routing process, use the **router bgp** command in global configuration mode. To remove a BGP routing process, use the **no** form of this command.

router bgp *autonomous-system-number*
no router bgp *autonomous-system-number*

Syntax Description	<i>autonomous-system-number</i>	Number of an autonomous system that identifies the router to other BGP routers and tags the routing information that is passed along. Number in the range from 1 to 65535.
---------------------------	---------------------------------	--

Command Default No BGP routing process is enabled by default.

Command Modes Global configuration (config)

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

Usage Guidelines This command allows you to set up a distributed routing core that automatically guarantees the loop-free exchange of routing information between autonomous systems.

Cisco has implemented the following two methods of representing autonomous system numbers:

- Asplain—Decimal value notation where both 2-byte and 4-byte autonomous system numbers are represented by their decimal value. For example, 65526 is a 2-byte autonomous system number and 234567 is a 4-byte autonomous system number.
- Asdot—Autonomous system dot notation where 2-byte autonomous system numbers are represented by their decimal value and 4-byte autonomous system numbers are represented by a dot notation. For example, 65526 is a 2-byte autonomous system number and 1.169031 is a 4-byte autonomous system number (this is dot notation for the 234567 decimal number).

For details about the third method of representing autonomous system numbers, see [RFC 5396](#).



Note

In Cisco IOS releases that include 4-byte ASN support, command accounting and command authorization that include a 4-byte ASN number are sent in the asplain notation irrespective of the format that is used on the command-line interface.

Asplain as Default Autonomous System Number Formatting

In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXH, Cisco IOS XE Release 2.4, and later releases, the Cisco implementation of 4-byte autonomous system numbers uses asplain as the default display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain and asdot format. In addition, the default format for matching 4-byte autonomous system numbers in regular expressions is asplain, so you must ensure that any regular expressions to match 4-byte autonomous system numbers are written in the asplain format. If you want to change the

default **show** command output to display 4-byte autonomous system numbers in the asdot format, use the **bgp asnotation dot** command under router configuration mode. When the asdot format is enabled as the default, any regular expressions to match 4-byte autonomous system numbers must be written using the asdot format, or the regular expression match will fail. The tables below show that although you can configure 4-byte autonomous system numbers in either asplain or asdot format, only one format is used to display **show** command output and control 4-byte autonomous system number matching for regular expressions, and the default is asplain format. To display 4-byte autonomous system numbers in **show** command output and to control matching for regular expressions in the asdot format, you must configure the **bgp asnotation dot** command. After enabling the **bgp asnotation dot** command, a hard reset must be initiated for all BGP sessions by entering the **clear ip bgp *** command.



Note If you are upgrading to an image that supports 4-byte autonomous system numbers, you can still use 2-byte autonomous system numbers. The **show** command output and regular expression match are not changed and remain in asplain (decimal value) format for 2-byte autonomous system numbers regardless of the format configured for 4-byte autonomous system numbers.

Table 130: Default Asplain 4-Byte Autonomous System Number Format

Format	Configuration Format	Show Command Output and Regular Expression Match Format
asplain	2-byte: 1 to 65535 4-byte: 65536 to 4294967295	2-byte: 1 to 65535 4-byte: 65536 to 4294967295
asdot	2-byte: 1 to 65535 4-byte: 1.0 to 65535.65535	2-byte: 1 to 65535 4-byte: 65536 to 4294967295

Table 131: Asdot 4-Byte Autonomous System Number Format

Format	Configuration Format	Show Command Output and Regular Expression Match Format
asplain	2-byte: 1 to 65535 4-byte: 65536 to 4294967295	2-byte: 1 to 65535 4-byte: 1.0 to 65535.65535
asdot	2-byte: 1 to 65535 4-byte: 1.0 to 65535.65535	2-byte: 1 to 65535 4-byte: 1.0 to 65535.65535

Reserved and Private Autonomous System Numbers

In Cisco IOS Release 12.0(32)S12, 12.0(32)SY8, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXH, 12.4(24)T, Cisco IOS XE Release 2.3 and later releases, the Cisco implementation of BGP supports RFC 4893. RFC 4893 was developed to allow BGP to support a gradual transition from 2-byte autonomous system numbers to 4-byte autonomous system numbers. A new reserved (private) autonomous system number, 23456, was created by RFC 4893 and this number cannot be configured as an autonomous system number in the Cisco IOS CLI.

RFC 5398, *Autonomous System (AS) Number Reservation for Documentation Use*, describes new reserved autonomous system numbers for documentation purposes. Use of the reserved numbers allow configuration examples to be accurately documented and avoids conflict with production networks if these configurations are literally copied. The reserved numbers are documented in the IANA autonomous system number registry. Reserved 2-byte autonomous system numbers are in the contiguous block, 64496 to 64511 and reserved 4-byte autonomous system numbers are from 65536 to 65551 inclusive.

Private 2-byte autonomous system numbers are still valid in the range from 64512 to 65534 with 65535 being reserved for special use. Private autonomous system numbers can be used for internal routing domains but must be translated for traffic that is routed out to the Internet. BGP should not be configured to advertise private autonomous system numbers to external networks. Cisco IOS software does not remove private autonomous system numbers from routing updates by default. Cisco recommends that ISPs filter private autonomous system numbers.

**Note**

Autonomous system number assignment for public and private networks is governed by the IANA. For information about autonomous system numbers, including reserved number assignment, or to apply to register an autonomous system number, see the following URL: <http://www.iana.org/>.

Examples

The following example shows how to configure a BGP process for autonomous system 45000 and configures two external BGP neighbors in different autonomous systems using 2-byte autonomous system numbers:

```
Device> enable
Device# configure terminal
Device(config)# router bgp 45000
Device(config-router)# neighbor 192.168.1.2 remote-as 40000
Device(config-router)# neighbor 192.168.3.2 remote-as 50000
Device(config-router)# neighbor 192.168.3.2 description finance
Device(config-router)# address-family ipv4
Device(config-router-af)# neighbor 192.168.1.2 activate
Device(config-router-af)# neighbor 192.168.3.2 activate
Device(config-router-af)# no auto-summary
Device(config-router-af)# no synchronization
Device(config-router-af)# network 172.17.1.0 mask 255.255.255.0
Device(config-router-af)# exit-address-family
```

The following example shows how to configure a BGP process for autonomous system 65538 and configures two external BGP neighbors in different autonomous systems using 4-byte autonomous system numbers in asplain notation. This example is supported in Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXH, Cisco IOS XE Release 2.4, and later releases.

```
Device> enable
Device# configure terminal
Device(config)# router bgp 65538
Device(config-router)# neighbor 192.168.1.2 remote-as 65536
Device(config-router)# neighbor 192.168.3.2 remote-as 65550
Device(config-router)# neighbor 192.168.3.2 description finance
Device(config-router)# address-family ipv4
Device(config-router-af)# neighbor 192.168.1.2 activate
Device(config-router-af)# neighbor 192.168.3.2 activate
Device(config-router-af)# no auto-summary
Device(config-router-af)# no synchronization
Device(config-router-af)# network 172.17.1.0 mask 255.255.255.0
Device(config-router-af)# exit-address-family
```

Related Commands

Command	Description
neighbor remote-as	Adds an entry to the BGP or multiprotocol BGP neighbor table.
network (BGP and multiprotocol BGP)	Specifies the list of networks for the BGP 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-number}virtual-instance-name}
no router eigrp {autonomous-system-number}virtual-instance-name}
```

Syntax Description	<i>autonomous-system-number</i>	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.
	<i>virtual-instance-name</i>	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 Everest 16.6.1	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 ospf

To configure an OSPF routing process, use the **router ospf** command in global configuration mode. To terminate an OSPF routing process, use the **no** form of this command.

```
router ospf process-id [vrf vrf-name]
```

no router ospf process-id [vrf vrf-name]

Syntax Description	<i>process-id</i>	Internally used identification parameter for an OSPF routing process. It is locally assigned and can be any positive integer. A unique value is assigned for each OSPF routing process.
	vrf <i>vrf-name</i>	(Optional) Specifies the name of the VPN routing and forwarding (VRF) instance to associate with OSPF VRF processes.

Command Default No OSPF routing process is defined.

Command Modes Global configuration

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines You can specify multiple OSPF routing processes in each router.

After you enter the **router ospf** command, you can enter the maximum number of paths. There can be from 1 to 32 paths.

Examples

The following example configures an OSPF routing process and assign a process number of 109:

```
Device(config)# router ospf 109
```

This example shows a basic OSPF configuration using the **router ospf** command to configure OSPF VRF instance processes for the VRFs first, second, and third:

```
Device> enable
Device# configure terminal
Device(config)# router ospf 12 vrf first
Device(config)# router ospf 13 vrf second
Device(config)# router ospf 14 vrf third
Device(config)# exit
```

The following example shows usage of the **maximum-paths** option:

```
Device> enable
Device# configure terminal
Device(config)# router ospf
Device(config-router)# maximum-paths 2
Device(config-router)# exit
```

Related Commands	Command	Description
	network area	Defines the interfaces on which OSPF runs and defines the area ID for those interfaces.

set community

To set the BGP communities attribute, use the **set community** route map configuration command. To delete the entry, use the **no** form of this command.

set community

```
set community {community-number [additive] [well-known-community] | none}
no set community
```

Syntax Description	<p><i>community-number</i> Specifies that community number. Valid values are from 1 to 4294967200, no-export, or no-advertise.</p> <p>additive (Optional) Adds the community to the already existing communities.</p> <p><i>well-known-community</i> (Optional) Well known communities can be specified by using the following keywords:</p> <ul style="list-style-type: none"> • internet • local-as • no-advertise • no-export <p>none (Optional) Removes the community attribute from the prefixes that pass the route map.</p>
---------------------------	--

Command Default No BGP communities attributes exist.

Command Modes Route-map configuration (config-route-map)

Table 132:

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines You must have a match clause (even if it points to a “permit everything” list) if you want to set tags.

Use the **route-map** global configuration command, and the **match** and **set** route map configuration commands, to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria* --the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the *set actions* --the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **set** route map configuration commands specify the redistribution *set actions* to be performed when all of the match criteria of a route map are met. When all match criteria are met, all set actions are performed.

Examples

In the following example, routes that pass the autonomous system path access list 1 have the community set to 109. Routes that pass the autonomous system path access list 2 have the community set to no-export (these routes will not be advertised to any external BGP [eBGP] peers).

```
route-map set_community 10 permit
match as-path 1
set community 109
route-map set_community 20 permit
```

```
match as-path 2
set community no-export
```

In the following similar example, routes that pass the autonomous system path access list 1 have the community set to 109. Routes that pass the autonomous system path access list 2 have the community set to local-as (the router will not advertise this route to peers outside the local autonomous system).

```
route-map set_community 10 permit
match as-path 1
set community 109
route-map set_community 20 permit
match as-path 2
set community local-as
```

Related Commands	Command	Description
	ip community-list	Creates a community list for BGP and control access to it.
	match community	Matches a BGP community.
	route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
	set comm-list delete	Removes communities from the community attribute of an inbound or outbound update.
	show ip bgp community	Displays routes that belong to specified BGP communities.

set ip next-hop (BGP)

To indicate where to output packets that pass a match clause of a route map for policy routing, use the **set ip next-hop** command in route-map configuration mode. To delete an entry, use the **no** form of this command.

```
set ip next-hop ip-address[{...ip-address}][{peer-address}]
no set ip next-hop ip-address[{...ip-address}][{peer-address}]
```

Syntax Description	<i>ip-address</i>	IP address of the next hop to which packets are output. It need not be an adjacent router.
	peer-address	(Optional) Sets the next hop to be the BGP peering address.

Command Default This command is disabled by default.

Command Modes Route-map configuration (config-route-map)

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

set ip next-hop (BGP)**Usage Guidelines**

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the *ip-address* argument.

Use the **ip policy route-map** interface configuration command, the **route-map** global configuration command, and the **match** and **set** route-map configuration commands to define the conditions for policy routing packets. The **ip policy route-map** command identifies a route map by name. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria* --the conditions under which policy routing occurs. The **set** commands specify the *set actions* --the particular routing actions to perform if the criteria enforced by the **match** commands are met.

If the first next hop specified with the **set ip next-hop** command is down, the optionally specified IP addresses are tried in turn.

When the **set ip next-hop** command is used with the **peer-address** keyword in an inbound route map of a BGP peer, the next hop of the received matching routes will be set to be the neighbor peering address, overriding any third-party next hops. So the same route map can be applied to multiple BGP peers to override third-party next hops.

When the **set ip next-hop** command is used with the **peer-address** keyword in an outbound route map of a BGP peer, the next hop of the advertised matching routes will be set to be the peering address of the local router, thus disabling the next hop calculation. The **set ip next-hop** command has finer granularity than the (per-neighbor) **neighbor next-hop-self** command, because you can set the next hop for some routes, but not others. The **neighbor next-hop-self** command sets the next hop for all routes sent to that neighbor.

The set clauses can be used in conjunction with one another. They are evaluated in the following order:

1. **set ip next-hop**
2. **set interface**
3. **set ip default next-hop**
4. **set default interface**

**Note**

To avoid a common configuration error for reflected routes, do not use the **set ip next-hop** command in a route map to be applied to BGP route reflector clients.

Configuring the **set ip next-hop ...ip-address** command on a VRF interface allows the next hop to be looked up in a specified VRF address family. In this context, the ...*ip-address* argument matches that of the specified VRF instance.

Examples

In the following example, three routers are on the same FDDI LAN (with IP addresses 10.1.1.1, 10.1.1.2, and 10.1.1.3). Each is in a different autonomous system. The **set ip next-hop peer-address** command specifies that traffic from the router (10.1.1.3) in remote autonomous system 300 for the router (10.1.1.1) in remote autonomous system 100 that matches the route map is passed through the router bgp 200, rather than sent directly to the router (10.1.1.1) in autonomous system 100 over their mutual connection to the LAN.

```
Device(config)#router bgp 200
Device(config)#neighbor 10.1.1.3 remote-as 300
Device(config)#neighbor 10.1.1.3 route-map set-peer-address out
Device(config)#neighbor 10.1.1.1 remote-as 100
```

```
Device(config)#route-map set-peer-address permit 10
Device(config)#set ip next-hop peer-address
```

Related Commands	Command	Description
	ip policy route-map	Identifies a route map to use for policy routing on an interface.
	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.
	match length	Bases policy routing on the Level 3 length of a packet.
	neighbor next-hop-self	Disables next hop processing of BGP updates on the router.
	route-map (IP)	Defines the conditions for redistributing routes from one routing protocol to another, or enables policy routing.
	set default interface	Indicates where to output packets that pass a match clause of a route map for policy routing and that have no explicit route to the destination.
	set interface	Indicates where to output packets that pass a match clause of a route map for policy routing.
	set ip default next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing and for which the Cisco IOS software has no explicit route to a destination.

show ip bgp

To display entries in the Border Gateway Protocol (BGP) routing table, use the **show ip bgp** command in user EXEC or privileged EXEC mode.

```
show ip bgp [{ip-address [{mask [{longer-prefixes [{injected}]} | shorter-prefixes [{length}]} | bestpath | multipaths | subnets}]] | bestpath | multipaths} | all | oer-paths | prefix-list name | pending-prefixes | route-map name | version {version-number | recent offset-value}}]
```

Syntax Description	Parameter	Description
	<i>ip-address</i>	(Optional) IP address entered to filter the output to display only a particular host or network in the BGP routing table.
	<i>mask</i>	(Optional) Mask to filter or match hosts that are part of the specified network.
	longer-prefixes	(Optional) Displays the specified route and all more-specific routes.
	injected	(Optional) Displays more-specific prefixes injected into the BGP routing table.
	shorter-prefixes	(Optional) Displays the specified route and all less-specific routes.
	<i>length</i>	(Optional) The prefix length. The range is a number from 0 to 32.
	bestpath	(Optional) Displays the best path for this prefix.

show ip bgp

multipaths	(Optional) Displays multipaths for this prefix.
subnets	(Optional) Displays the subnet routes for the specified prefix.
all	(Optional) Displays all address family information in the BGP routing table.
oer-paths	(Optional) Displays Optimized Edge Routing (OER) controlled prefixes in the BGP routing table.
prefix-list <i>name</i>	(Optional) Filters the output based on the specified prefix list.
pending-prefixes	(Optional) Displays prefixes that are pending deletion from the BGP routing table.
route-map <i>name</i>	(Optional) Filters the output based on the specified route map.
version <i>version-number</i>	(Optional) Displays all prefixes with network versions greater than or equal to the specified version number. The range is from 1 to 4294967295.
recent <i>offset-value</i>	(Optional) Displays the offset from the current routing table version. The range is from 1 to 4294967295.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Table 133:

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines

The **show ip bgp** command is used to display the contents of the BGP routing table. The output can be filtered to display entries for a specific prefix, prefix length, and prefixes injected through a prefix list, route map, or conditional advertisement.

When changes are made to the network address, the network version number is incremented. Use the **version** keyword to view a specific network version.

In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX1, Cisco IOS XE Release 2.4, and later releases, 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 followed by the **clear ip bgp *** command to perform a hard reset of all current BGP sessions.

In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, the Cisco implementation of 4-byte autonomous system numbers uses asdot—1.2, for example—as the only configuration format, regular expression match, and output display, with no asplain support.

oer-paths Keyword

In Cisco IOS Release 12.3(8)T and later releases, BGP prefixes that are monitored and controlled by OER are displayed by entering the **show ip bgp** command with the **oer-paths** keyword.

show ip bgp: Example

The following sample output displays the BGP routing table:

```
Device# show ip bgp
```

```
BGP table version is 6, local router ID is 10.0.96.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, x best-external, f
              RT-Filter, a additional-path
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found
```

	Network	Next Hop	Metric	LocPrf	Weight	Path
N*	10.0.0.1	10.0.0.3	0		0	3 ?
N*>		10.0.3.5	0		0	4 ?
Nr	10.0.0.0/8	10.0.0.3	0		0	3 ?
Nr>		10.0.3.5	0		0	4 ?
Nr>	10.0.0.0/24	10.0.0.3	0		0	3 ?
V*>	10.0.2.0/24	0.0.0.0	0		32768	i
Vr>	10.0.3.0/24	10.0.3.5	0		0	4 ?

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

Table 134: show ip bgp Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.

show ip bgp

Field	Description
Status codes	<p>Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values:</p> <ul style="list-style-type: none"> • s—The table entry is suppressed. • d—The table entry is dampened. • h—The table entry history. • *—The table entry is valid. • >—The table entry is the best entry to use for that network. • i—The table entry was learned via an internal BGP (iBGP) session. • r—The table entry is a RIB-failure. • S—The table entry is stale. • m—The table entry has multipath to use for that network. • b—The table entry has a backup path to use for that network. • x—The table entry has a best external route to use for the network.
Origin codes	<p>Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values:</p> <ul style="list-style-type: none"> • a—Path is selected as an additional path. • i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. • e—Entry originated from an Exterior Gateway Protocol (EGP). • ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
RPKI validation codes	If shown, the RPKI validation state for the network prefix, which is downloaded from the RPKI server. The codes are shown only if the bgp rpki server or neighbor announce rpki state command is configured.
Network	IP address of a network entity.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.
Metric	If shown, the value of the interautonomous system metric.
LocPrf	Local preference value as set with the set local-preference route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.

Field	Description
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.
(stale)	Indicates that the following path for the specified autonomous system is marked as "stale" during a graceful restart process.

show ip bgp (4-Byte Autonomous System Numbers): Example

The following sample output shows the BGP routing table with 4-byte autonomous system numbers, 65536 and 65550, shown under the Path field. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXII, Cisco IOS XE Release 2.4, or a later release.

```
Device# show ip bgp
```

```
BGP table version is 4, local router ID is 172.16.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.1.0/24    192.168.1.2        0          0 65536   i
*> 10.2.2.0/24    192.168.3.2        0          0 65550   i
*> 172.16.1.0/24  0.0.0.0           0          32768   i
```

show ip bgp network: Example

The following sample output displays information about the 192.168.1.0 entry in the BGP routing table:

```
Device# show ip bgp 192.168.1.0
```

```
BGP routing table entry for 192.168.1.0/24, version 22
Paths: (2 available, best #2, table default)
      Additional-path
      Advertised to update-groups:
          3
          10 10
          192.168.3.2 from 172.16.1.2 (10.2.2.2)
              Origin IGP, metric 0, localpref 100, valid, internal, backup/repair
          10 10
          192.168.1.2 from 192.168.1.2 (10.3.3.3)
              Origin IGP, localpref 100, valid, external, best , recursive-via-connected
```

The following sample output displays information about the 10.3.3.3 255.255.255.255 entry in the BGP routing table:

```
Device# show ip bgp 10.3.3.3 255.255.255.255
```

```
BGP routing table entry for 10.3.3.3/32, version 35
Paths: (3 available, best #2, table default)
      Multipath: eBGP
      Flag: 0x860
      Advertised to update-groups:
          1
          200
```

show ip bgp

```

10.71.8.165 from 10.71.8.165 (192.168.0.102)
  Origin incomplete, localpref 100, valid, external, backup/repair
    Only allowed to recurse through connected route
200
  10.71.11.165 from 10.71.11.165 (192.168.0.102)
    Origin incomplete, localpref 100, weight 100, valid, external, best
      Only allowed to recurse through connected route
200
  10.71.10.165 from 10.71.10.165 (192.168.0.104)
    Origin incomplete, localpref 100, valid, external,
      Only allowed to recurse through connected route

```

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

Table 135: show ip bgp ip-address Field Descriptions

Field	Description
BGP routing table entry for	IP address or network number of the routing table entry.
version	Internal version number of the table. This number is incremented whenever the table changes.
Paths	The number of available paths, and the number of installed best paths. This line displays “Default-IP-Routing-Table” when the best path is installed in the IP routing table.
Multipath	This field is displayed when multipath load sharing is enabled. This field will indicate if the multipaths are iBGP or eBGP.
Advertised to update-groups	The number of each update group for which advertisements are processed.
Origin	Origin of the entry. The origin can be IGP, EGP, or incomplete. This line displays the configured metric (0 if no metric is configured), the local preference value (100 is default), and the status and type of route (internal, external, multipath, best).
Extended Community	This field is displayed if the route carries an extended community attribute. The attribute code is displayed on this line. Information about the extended community is displayed on a subsequent line.

show ip bgp all: Example

The following is sample output from the **show ip bgp** command entered with the **all** keyword. Information about all configured address families is displayed.

```

Device# show ip bgp all

For address family: IPv4 Unicast  *****
BGP table version is 27, local router ID is 10.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure
Origin codes: i - IGP, e - EGP, ? - incomplete
      Network          Next Hop          Metric LocPrf Weight Path
  *> 10.1.1.0/24      0.0.0.0            0       32768  ?
  *> 10.13.13.0/24   0.0.0.0            0       32768  ?

```

```

*> 10.15.15.0/24      0.0.0.0          0      32768 ?
*>i10.18.18.0/24    172.16.14.105   1388  91351      0 100 e
*>i10.100.0.0/16    172.16.14.107   262    272      0 1 2 3 i
*>i10.100.0.0/16    172.16.14.105   1388  91351      0 100 e
*>i10.101.0.0/16    172.16.14.105   1388  91351      0 100 e
*>i10.103.0.0/16    172.16.14.101   1388  173      173 100 e
*>i10.104.0.0/16    172.16.14.101   1388  173      173 100 e
*>i10.100.0.0/16    172.16.14.106   2219  20889      0 53285 33299 51178 47751 e
*>i10.101.0.0/16    172.16.14.106   2219  20889      0 53285 33299 51178 47751 e
* 10.100.0.0/16     172.16.14.109   2309          0 200 300 e
*> 172.16.14.108    172.16.14.108   1388          0 100 e
* 10.101.0.0/16     172.16.14.109   2309          0 200 300 e
*> 172.16.14.108    172.16.14.108   1388          0 100 e
*> 10.102.0.0/16    172.16.14.108   1388          0 100 e
*> 172.16.14.0/24   0.0.0.0          0      32768 ?
*> 192.168.5.0      0.0.0.0          0      32768 ?
*> 10.80.0.0/16     172.16.14.108   1388          0 50 e
*> 10.80.0.0/16     172.16.14.108   1388          0 50 e
For address family: VPNv4 Unicast *****
BGP table version is 21, local router ID is 10.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure
Origin codes: i - IGP, e - EGP, ? - incomplete
Network      Next Hop          Metric LocPrf Weight Path
Route Distinguisher: 1:1 (default for vrf vpn1)
*> 10.1.1.0/24   192.168.4.3      1622          0 100 53285 33299 51178
{27016,57039,16690} e
*> 10.1.2.0/24   192.168.4.3      1622          0 100 53285 33299 51178
{27016,57039,16690} e
*> 10.1.3.0/24   192.168.4.3      1622          0 100 53285 33299 51178
{27016,57039,16690} e
*> 10.1.4.0/24   192.168.4.3      1622          0 100 53285 33299 51178
{27016,57039,16690} e
*> 10.1.5.0/24   192.168.4.3      1622          0 100 53285 33299 51178
{27016,57039,16690} e
*>i172.17.1.0/24 10.3.3.3        10      30      0 53285 33299 51178 47751 ?
*>i172.17.2.0/24 10.3.3.3        10      30      0 53285 33299 51178 47751 ?
*>i172.17.3.0/24 10.3.3.3        10      30      0 53285 33299 51178 47751 ?
*>i172.17.4.0/24 10.3.3.3        10      30      0 53285 33299 51178 47751 ?
*>i172.17.5.0/24 10.3.3.3        10      30      0 53285 33299 51178 47751 ?
For address family: IPv4 Multicast *****
BGP table version is 11, local router ID is 10.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure
Origin codes: i - IGP, e - EGP, ? - incomplete
Network      Next Hop          Metric LocPrf Weight Path
*> 10.40.40.0/26   172.16.14.110   2219          0 21 22 {51178,47751,27016} e
* 10.1.1.1          1622          0 15 20 1 {2} e
*> 10.40.40.64/26  172.16.14.110   2219          0 21 22 {51178,47751,27016} e
* 10.1.1.1          1622          0 15 20 1 {2} e
*> 10.40.40.128/26 172.16.14.110   2219          0 21 22 {51178,47751,27016} e
* 10.1.1.1          2563          0 15 20 1 {2} e
*> 10.40.40.192/26 10.1.1.1        2563          0 15 20 1 {2} e
*> 10.40.41.0/26   10.1.1.1        1209          0 15 20 1 {2} e
*>i10.102.0.0/16   10.1.1.1        300           500      0 5 4 {101,102} e
*>i10.103.0.0/16   10.1.1.1        300           500      0 5 4 {101,102} e
For address family: NSAP Unicast *****
BGP table version is 1, local router ID is 10.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure
Origin codes: i - IGP, e - EGP, ? - incomplete
Network      Next Hop          Metric LocPrf Weight Path
* i45.0000.0002.0001.000c.00  49.0001.0000.0000.0a00          100      0 ?
* i46.0001.0000.0000.0000.0a00 49.0001.0000.0000.0a00          100      0 ?

```

show ip bgp

* i47.0001.0000.0000.000b.00	49.0001.0000.0000.0a00	100	0 ?
* i47.0001.0000.0000.000e.00	49.0001.0000.0000.0a00		

show ip bgp longer-prefixes: Example

The following is sample output from the **show ip bgp longer-prefixes** command:

```
Device# show ip bgp 10.92.0.0 255.255.0.0 longer-prefixes

BGP table version is 1738, local router ID is 192.168.72.24
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
      Network          Next Hop      Metric LocPrf Weight Path
*-> 10.92.0.0        10.92.72.30    8896     32768 ?
*           10.92.72.30
*-> 10.92.1.0        10.92.72.30    8796     32768 ?
*           10.92.72.30
*-> 10.92.11.0       10.92.72.30   42482     32768 ?
*           10.92.72.30
*-> 10.92.14.0       10.92.72.30    8796     32768 ?
*           10.92.72.30
*-> 10.92.15.0       10.92.72.30    8696     32768 ?
*           10.92.72.30
*-> 10.92.16.0       10.92.72.30   1400     32768 ?
*           10.92.72.30
*-> 10.92.17.0       10.92.72.30   1400     32768 ?
*           10.92.72.30
*-> 10.92.18.0       10.92.72.30   8876     32768 ?
*           10.92.72.30
*-> 10.92.19.0       10.92.72.30   8876     32768 ?
*           10.92.72.30
```

show ip bgp shorter-prefixes: Example

The following is sample output from the **show ip bgp shorter-prefixes** command. An 8-bit prefix length is specified.

```
Device# show ip bgp 172.16.0.0/16 shorter-prefixes 8

*> 172.16.0.0        10.0.0.2          0 ??
*           10.0.0.2          0 200 ?
```

show ip bgp prefix-list: Example

The following is sample output from the **show ip bgp prefix-list** command:

```
Device# show ip bgp prefix-list ROUTE

BGP table version is 39, local router ID is 10.0.0.1
Status codes:s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes:i - IGP, e - EGP, ? - incomplete
      Network          Next Hop      Metric LocPrf Weight Path
*> 192.168.1.0       10.0.0.2          0 ??
*           10.0.0.2          0 200 ?
```

show ip bgp route-map: Example

The following is sample output from the **show ip bgp route-map** command:

```
Device# show ip bgp route-map LEARNED_PATH

BGP table version is 40, local router ID is 10.0.0.1
Status codes:s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes:i - IGP, e - EGP, ? - incomplete
      Network          Next Hop          Metric LocPrf Weight Path
* > 192.168.1.0      10.0.0.2            0       ?           0 200 ?
*                  10.0.0.2            0       ?           0 200 ?
```

show ip bgp (Additional Paths): Example

The following output indicates (for each neighbor) whether any of the additional path tags (group-best, all, best 2 or best 3) are applied to the path. A line of output indicates rx pathid (received from neighbor) and tx pathid (announcing to neighbors). Note that the “Path advertised to update-groups:” is now per-path when the BGP Additional Paths feature is enabled.

```
Device# show ip bgp 10.0.0.1 255.255.255.224

BGP routing table entry for 10.0.0.1/28, version 82
Paths: (10 available, best #5, table default)
  Path advertised to update-groups:
    21          25
    Refresh Epoch 1
    20 50, (Received from a RR-client)
      192.0.2.1 from 192.0.2.1 (192.0.2.1)
        Origin IGP, metric 200, localpref 100, valid, internal, all
        Originator: 192.0.2.1, Cluster list: 2.2.2.2
        mpls labels in/out 16/nolabel
        rx pathid: 0, tx pathid: 0x9
  Path advertised to update-groups:
    18          21
    Refresh Epoch 1
    30
      192.0.2.2 from 192.0.2.2 (192.0.2.2)
        Origin IGP, metric 200, localpref 100, valid, internal, group-best, all
        Originator: 192.0.2.2, Cluster list: 4.4.4.4
        mpls labels in/out 16/nolabel
        rx pathid: 0x1, tx pathid: 0x8
  Path advertised to update-groups:
    16          18          19          20          21          22          24
    25          27
    Refresh Epoch 1
    10
      192.0.2.3 from 192.0.2.3 (192.0.2.3)
        Origin IGP, metric 200, localpref 100, valid, external, best2, all
        mpls labels in/out 16/nolabel
        rx pathid: 0, tx pathid: 0x7
  Path advertised to update-groups:
    20          21          22          24          25
    Refresh Epoch 1
    10
      192.0.2.4 from 192.0.2.4 (192.0.2.4)
        Origin IGP, metric 300, localpref 100, valid, external, best3, all
        mpls labels in/out 16/nolabel
        rx pathid: 0, tx pathid: 0x6
  Path advertised to update-groups:
```

show ip bgp

```

      10          13          17          18          19          20          21
      22          23          24          25          26          27          28
Refresh Epoch 1
10
  192.0.2.5 from 192.0.2.5 (192.0.2.5)
    Origin IGP, metric 100, localpref 100, valid, external, best
    mpls labels in/out 16/nolabel
    rx pathid: 0, tx pathid: 0x0
Path advertised to update-groups:
  21
Refresh Epoch 1
30
  192.0.2.6 from 192.0.2.6 (192.0.2.6)
    Origin IGP, metric 200, localpref 100, valid, internal, all
    Originator: 192.0.2.6, Cluster list: 5.5.5.5
    mpls labels in/out 16/nolabel
    rx pathid: 0x1, tx pathid: 0x5
Path advertised to update-groups:
  18          23          24          26          28
Refresh Epoch 1
60 40, (Received from a RR-client)
  192.0.2.7 from 192.0.2.7 (192.0.2.7)
    Origin IGP, metric 250, localpref 100, valid, internal, group-best
    Originator: 192.0.2.7, Cluster list: 3.3.3.3
    mpls labels in/out 16/nolabel
    rx pathid: 0x2, tx pathid: 0x2
Path advertised to update-groups:
  25
Refresh Epoch 1
30 40, (Received from a RR-client)
  192.0.2.8 from 192.0.2.8 (192.0.2.8)
    Origin IGP, metric 200, localpref 100, valid, internal, all
    Originator: 192.0.2.8, Cluster list: 2.2.2.2
    mpls labels in/out 16/nolabel
    rx pathid: 0x1, tx pathid: 0x3
Path advertised to update-groups:
  18          21          23          24          25          26          28
Refresh Epoch 1
20 40, (Received from a RR-client)
  192.0.2.9 from 192.0.2.9 (192.0.2.9)
    Origin IGP, metric 200, localpref 100, valid, internal, group-best, all
    Originator: 192.0.2.9, Cluster list: 2.2.2.2
    mpls labels in/out 16/nolabel
    rx pathid: 0x1, tx pathid: 0x4
Path advertised to update-groups:
  21
Refresh Epoch 1
30 40
  192.0.2.9 from 192.0.2.9 (192.0.2.9)
    Origin IGP, metric 100, localpref 100, valid, internal, all
    Originator: 192.0.2.9, Cluster list: 4.4.4.4
    mpls labels in/out 16/nolabel
    rx pathid: 0x1, tx pathid: 0x1

```

show ip bgp network (BGP Attribute Filter): Example

The following is sample output from the **show ip bgp** command that displays unknown and discarded path attributes:

```

Device# show ip bgp 192.0.2.0/32
BGP routing table entry for 192.0.2.0/32, version 0

```

```

Paths: (1 available, no best path)
  Refresh Epoch 1
    Local
      192.168.101.2 from 192.168.101.2 (192.168.101.2)
        Origin IGP, localpref 100, valid, internal
        unknown transitive attribute: flag 0xE0 type 0x81 length 0x20
          value 0000 0000 0000 0000 0000 0000 0000
          0000 0000 0000 0000 0000 0000 0000

        unknown transitive attribute: flag 0xE0 type 0x83 length 0x20
          value 0000 0000 0000 0000 0000 0000 0000
          0000 0000 0000 0000 0000 0000 0000

        discarded unknown attribute: flag 0x40 type 0x63 length 0x64
          value 0000 0000 0000 0000 0000 0000 0000
          0000 0000 0000 0000 0000 0000 0000

```

show ip bgp version: Example

The following is sample output from the **show ip bgp version** command:

```
Device# show ip bgp version
```

```

BGP table version is 5, local router ID is 10.2.4.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete
Network Next Hop Metric LocPrf Weight Path
*> 192.168.34.2/24 10.0.0.1 0 0 1 ?
*> 192.168.35.2/24 10.0.0.1 0 0 1 ?

```

The following example shows how to display the network version:

```
Device# show ip bgp 192.168.34.2 | include version
```

```
BGP routing table entry for 192.168.34.2/24, version 5
```

The following sample output from the **show ip bgp version recent** command displays the prefix changes in the specified version:

```
Device# show ip bgp version recent 2
```

```

BGP table version is 5, local router ID is 10.2.4.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete

```

Network	Next Hop	Metric	LocPrf	Weight	Path
*> 192.168.134.1/28	10.0.0.1	0	0	1	?
*> 192.168.134.19/28	10.0.0.1	0	0	1	?
*> 192.168.134.34/28	10.0.0.1	0	0	1	?

Related Commands

Command	Description
bgp asnotation dot	Changes the default display and the regular expression match format of BGP 4-byte autonomous system numbers from asplain (decimal values) to dot notation.

show ip bgp neighbors

Command	Description
clear ip bgp	Resets BGP connections using hard or soft reconfiguration.
ip bgp community new-format	Configures BGP to display communities in the format AA:NN.
ip prefix-list	Creates a prefix list or adds a prefix-list entry.
route-map	Defines the conditions for redistributing routes from one routing protocol into another routing protocol.
router bgp	Configures the BGP routing process.

show ip bgp neighbors

To display information about Border Gateway Protocol (BGP) and TCP connections to neighbors, use the **show ip bgp neighbors** command in user or privileged EXEC mode.

```
show ip bgp [{ipv4 {multicast|unicast} | vpnv4 all | vpnv6 unicast all}] neighbors [{slowip-address | ipv6-address [{advertiseds-routes | dampened-routes | flap-statistics | paths [reg-exp] | policy [detail] | received prefix-filter | received-routes | routes}]}]
```

Syntax Description	ipv4	(Optional) Displays peers in the IPv4 address family.
	multicast	(Optional) Specifies IPv4 multicast address prefixes.
	unicast	(Optional) Specifies IPv4 unicast address prefixes.
	vpnv4 all	(Optional) Displays peers in the Vpnv4 address family.
	vpnv6 unicast all	(Optional) Displays peers in the Vpnv6 address family.
	slow	(Optional) Displays information about dynamically configured slow peers.
	<i>ip-address</i>	(Optional) IP address of the IPv4 neighbor. If this argument is omitted, information about all neighbors is displayed.
	<i>ipv6-address</i>	(Optional) IP address of the IPv6 neighbor.
	advertiseds-routes	(Optional) Displays all routes that have been advertised to neighbors.
	dampened-routes	(Optional) Displays the dampened routes received from the specified neighbor.
	flap-statistics	(Optional) Displays the flap statistics of the routes learned from the specified neighbor (for external BGP peers only).
	paths reg-exp	(Optional) Displays autonomous system paths learned from the specified neighbor. An optional regular expression can be used to filter the output.
	policy	(Optional) Displays the policies applied to this neighbor per address family.

detail	(Optional) Displays detailed policy information such as route maps, prefix lists, community lists, access control lists (ACLs), and autonomous system path filter lists.
received prefix-filter	(Optional) Displays the prefix list (outbound route filter [ORF]) sent from the specified neighbor.
received-routes	(Optional) Displays all received routes (both accepted and rejected) from the specified neighbor.
routes	(Optional) Displays all routes that are received and accepted. The output displayed when this keyword is entered is a subset of the output displayed by the received-routes keyword.

Command Default The output of this command displays information for all neighbors.

Command Modes User EXEC (>)

Privileged EXEC (#)

Command History *Table 136:*

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced.

Mainline and T Release	Modification
10.0	This command was introduced.
11.2	This command was modified. The received-routes keyword was added.
12.2(4)T	This command was modified. The received and prefix-filter keywords were added.
12.2(15)T	This command was modified. Support for the display of BGP graceful restart capability information was added.
12.3(7)T	This command was modified. The command output was modified to support the BGP TTL Security Check feature and to display explicit-null label information.
12.4(4)T	This command was modified. Support for the display of Bidirectional Forwarding Detection (BFD) information was added.
12.4(11)T	This command was modified. Support for the policy and detail keywords was added.
12.4(20)T	This command was modified. The output was modified to support BGP TCP path MTU discovery.
12.4(24)T	This command was modified. Support for displaying 4-byte autonomous system numbers in asdot notation was added.

show ip bgp neighbors

S Release	Modification
12.0(18)S	This command was modified. The output was modified to display the no-prepend configuration option.
12.0(21)ST	This command was modified. The output was modified to display Multiprotocol Label Switching (MPLS) label information.
12.0(22)S	This command was modified. Support for the display of BGP graceful restart capability information was added. Support for the Cisco 12000 series routers (Engine 0 and Engine 2) was also added.
12.0(25)S	This command was modified. The policy and detail keywords were added.
12.0(27)S	This command was modified. The command output was modified to support the BGP TTL Security Check feature and to display explicit-null label information.
12.0(31)S	This command was modified. Support for the display of BFD information was added.
12.0(32)S12	This command was modified. Support for displaying 4-byte autonomous system numbers in asdot notation was added.
12.0(32)SY8	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain notation was added and the default display format became asplain.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(17b)SXА	This command was integrated into Cisco IOS Release 12.2(17b)SXА.
12.2(18)SXE	This command was modified. Support for the display of BFD information was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was modified. The output was modified to support BGP TCP path Maximum Transmission Unit (MTU) discovery.
12.2(33)SRB	This command was modified. Support for the policy and detail keywords was added.
12.2(33)SXH	This command was modified. Support for displaying BGP dynamic neighbor information was added.
12.2(33)SRC	This command was modified. Support for displaying BGP graceful restart information was added.
12.2(33)SB	This command was modified. Support for displaying BFD and the BGP graceful restart per peer information was added, and support for the policy and detail keywords was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXII	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.

S Release	Modification
12.2(33)SRE	This command was modified. Support for displaying BGP best external and BGP additional path features information was added. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
15.0(1)S	This command was modified. The slow keyword was added.
15.0(1)SY	This command was integrated into Cisco IOS Release 15.0(1)SY.
15.1(1)S	This command was modified. The Layer 2 VPN address family is displayed if graceful restart or nonstop forwarding (NSF) is enabled.
15.1(1)SG	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain notation was added and the default display format became asplain.
15.2(4)S	This command was modified and implemented on the Cisco 7200 series router. The configured discard and treat-as-withdraw attributes are displayed, along with counts of incoming Updates with a matching discard attribute or treat-as-withdraw attribute, and number of times a malformed Update is treat-as-withdraw. The capabilities of the neighbor to send and receive additional paths that are advertised or received are added.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.
15.2(1)E	This command was integrated into Cisco IOS Release 15.2(1)E.

Cisco IOS XE	Modification
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
Cisco IOS XE Release 2.4	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain notation was added and the default display format became asplain.
Cisco IOS XE Release 3.1S	This command was modified. The slow keyword was added.
Cisco IOS XE Release 3.6S	This command was modified. Support for displaying BGP BFD multihop and C-bit information was added.
Cisco IOS XE Release 3.3SG	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain notation was added and the default display format became asplain.
Cisco IOS XE Release 3.7S	This command was implemented on the Cisco ASR 903 router and the output modified. The configured discard and treat-as-withdraw attributes are displayed, along with counts of incoming Updates with a matching discard attribute or treat-as-withdraw attribute, and number of times a malformed Update is treat-as-withdraw. The capabilities of the neighbor to send and receive additional paths that are advertised or received are added.

show ip bgp neighbors

Cisco IOS XE	Modification
Cisco IOS XE Release 3.8S	This command was modified. In support of the BGP Multi-Cluster ID feature, the cluster ID of a neighbor is displayed if the neighbor is assigned a cluster.

Usage Guidelines

Use the **show ip bgp neighbors** command to display BGP and TCP connection information for neighbor sessions. For BGP, this includes detailed neighbor attribute, capability, path, and prefix information. For TCP, this includes statistics related to BGP neighbor session establishment and maintenance.

Prefix activity is displayed based on the number of prefixes that are advertised and withdrawn. Policy denials display the number of routes that were advertised but then ignored based on the function or attribute that is displayed in the output.

In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases, 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 followed by the **clear ip bgp *** command to perform a hard reset of all current BGP sessions.

In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, the Cisco implementation of 4-byte autonomous system numbers uses asdot—1.2 for example—as the only configuration format, regular expression match, and output display, with no asplain support.

Cisco IOS Releases 12.0(25)S, 12.4(11)T, 12.2(33)SRB, 12.2(33)SB, and Later Releases

When BGP neighbors use multiple levels of peer templates, determining which policies are applied to the neighbor can be difficult.

In Cisco IOS Release 12.0(25)S, 12.4(11)T, 12.2(33)SRB, 12.2(33)SB, and later releases, the **policy** and **detail** keywords were added to display the inherited policies and the policies configured directly on the specified neighbor. Inherited policies are policies that the neighbor inherits from a peer group or a peer policy template.

Examples

Example output is different for the various keywords available for the **show ip bgp neighbors** command. Examples using the various keywords appear in the following sections.

show ip bgp neighbors: Example

The following example shows output for the BGP neighbor at 10.108.50.2. This neighbor is an internal BGP (iBGP) peer. This neighbor supports the route refresh and graceful restart capabilities.

```
Device# show ip bgp neighbors 10.108.50.2
BGP neighbor is 10.108.50.2, remote AS 1, internal link
BGP version 4, remote router ID 192.168.252.252
BGP state = Established, up for 00:24:25
Last read 00:00:24, last write 00:00:24, hold time is 180, keepalive interval is
60 seconds
Neighbor capabilities:
  Route refresh: advertised and received(old & new)
  MPLS Label capability: advertised and received
```

```

Graceful Restart Capability: advertised
Address family IPv4 Unicast: advertised and received
Message statistics:
  InQ depth is 0
  OutQ depth is 0
      Sent      Rcvd
  Opens:        3        3
  Notifications: 0        0
  Updates:      0        0
  Keepalives:   113     112
  Route Refresh: 0        0
  Total:       116     115
Default minimum time between advertisement runs is 5 seconds
For address family: IPv4 Unicast
  BGP additional-paths computation is enabled
  BGP advertise-best-external is enabled
  BGP table version 1, neighbor version 1/0
Output queue size : 0
  Index 1, Offset 0, Mask 0x2
  1 update-group member
      Sent      Rcvd
Prefix activity:      ----      ----
  Prefixes Current:    0        0
  Prefixes Total:      0        0
  Implicit Withdraw:  0        0
  Explicit Withdraw:  0        0
  Used as bestpath:   n/a      0
  Used as multipath:  n/a      0
      Outbound      Inbound
Local Policy Denied Prefixes:  -----      -----
  Total:                0        0
Number of NLIRIs in the update sent: max 0, min 0
Connections established 3; dropped 2
Last reset 00:24:26, due to Peer closed the session
External BGP neighbor may be up to 2 hops away.
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Connection is ECN Disabled
Local host: 10.108.50.1, Local port: 179
Foreign host: 10.108.50.2, Foreign port: 42698
Enqueued packets for retransmit: 0, input: 0 mis-ordered: 0 (0 bytes)
Event Timers (current time is 0x68B944):
  Timer      Starts      Wakeups      Next
  Retrans      27          0        0x0
  TimeWait      0          0        0x0
  AckHold      27         18        0x0
  SendWnd      0          0        0x0
  KeepAlive      0          0        0x0
  GiveUp        0          0        0x0
  PmtuAger      0          0        0x0
  DeadWait      0          0        0x0
iss: 3915509457 snduna: 3915510016 sndnxt: 3915510016 sndwnd: 15826
irs: 233567076 rcvnx: 233567616 rcvwnd: 15845 delrcvwnd: 539
SRTT: 292 ms, RTTO: 359 ms, RTV: 67 ms, KRTT: 0 ms
minRTT: 12 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: passive open, nagle, gen tcbs
IP Precedence value : 6
Datagrams (max data segment is 1460 bytes):
Rcvd: 38 (out of order: 0), with data: 27, total data bytes: 539
Sent: 45 (retransmit: 0, fastretransmit: 0, partialack: 0, Second Congestion: 08

```

The table below describes the significant fields shown in the display. Fields that are preceded by the asterisk character (*) are displayed only when the counter has a nonzero value.

show ip bgp neighbors

Table 137: show ip bgp neighbors Field Descriptions

Field	Description
BGP neighbor	IP address of the BGP neighbor and its autonomous system number.
remote AS	Autonomous system number of the neighbor.
local AS 300 no-prepend (not shown in display)	Verifies that the local autonomous system number is not prepended to received external routes. This output supports the hiding of the local autonomous systems when a network administrator is migrating autonomous systems.
internal link	“internal link” is displayed for iBGP neighbors; “external link” is displayed for external BGP (eBGP) neighbors.
BGP version	BGP version being used to communicate with the remote router.
remote router ID	IP address of the neighbor.
BGP state	Finite state machine (FSM) stage of session negotiation.
up for	Time, in hh:mm:ss, that the underlying TCP connection has been in existence.
Last read	Time, in hh:mm:ss, since BGP last received a message from this neighbor.
last write	Time, in hh:mm:ss, since BGP last sent a message to this neighbor.
hold time	Time, in seconds, that BGP will maintain the session with this neighbor without receiving messages.
keepalive interval	Time interval, in seconds, at which keepalive messages are transmitted to this neighbor.
Neighbor capabilities	BGP capabilities advertised and received from this neighbor. “advertised and received” is displayed when a capability is successfully exchanged between two routers.
Route refresh	Status of the route refresh capability.
MPLS Label capability	Indicates that MPLS labels are both sent and received by the eBGP peer.
Graceful Restart Capability	Status of the graceful restart capability.
Address family IPv4 Unicast	IP Version 4 unicast-specific properties of this neighbor.
Message statistics	Statistics organized by message type.
InQ depth is	Number of messages in the input queue.
OutQ depth is	Number of messages in the output queue.
Sent	Total number of transmitted messages.

Field	Description
Revd	Total number of received messages.
Opens	Number of open messages sent and received.
Notifications	Number of notification (error) messages sent and received.
Updates	Number of update messages sent and received.
Keepalives	Number of keepalive messages sent and received.
Route Refresh	Number of route refresh request messages sent and received.
Total	Total number of messages sent and received.
Default minimum time between...	Time, in seconds, between advertisement transmissions.
For address family:	Address family to which the following fields refer.
BGP table version	Internal version number of the table. This is the primary routing table with which the neighbor has been updated. The number increments when the table changes.
neighbor version	Number used by the software to track prefixes that have been sent and those that need to be sent.
1 update-group member	Number of the update-group member for this address family.
Prefix activity	Prefix statistics for this address family.
Prefixes Current	Number of prefixes accepted for this address family.
Prefixes Total	Total number of received prefixes.
Implicit Withdraw	Number of times that a prefix has been withdrawn and readvertised.
Explicit Withdraw	Number of times that a prefix has been withdrawn because it is no longer feasible.
Used as bestpath	Number of received prefixes installed as best paths.
Used as multipath	Number of received prefixes installed as multipaths.
* Saved (soft-reconfig)	Number of soft resets performed with a neighbor that supports soft reconfiguration. This field is displayed only if the counter has a nonzero value.
* History paths	This field is displayed only if the counter has a nonzero value.
* Invalid paths	Number of invalid paths. This field is displayed only if the counter has a nonzero value.
Local Policy Denied Prefixes	Prefixes denied due to local policy configuration. Counters are updated for inbound and outbound policy denials. The fields under this heading are displayed only if the counter has a nonzero value.

show ip bgp neighbors

Field	Description
* route-map	Displays inbound and outbound route-map policy denials.
* filter-list	Displays inbound and outbound filter-list policy denials.
* prefix-list	Displays inbound and outbound prefix-list policy denials.
* Ext Community	Displays only outbound extended community policy denials.
* AS_PATH too long	Displays outbound AS_PATH length policy denials.
* AS_PATH loop	Displays outbound AS_PATH loop policy denials.
* AS_PATH confed info	Displays outbound confederation policy denials.
* AS_PATH contains AS 0	Displays outbound denials of autonomous system 0.
* NEXT_HOP Martian	Displays outbound martian denials.
* NEXT_HOP non-local	Displays outbound nonlocal next-hop denials.
* NEXT_HOP is us	Displays outbound next-hop-self denials.
* CLUSTER_LIST loop	Displays outbound cluster-list loop denials.
* ORIGINATOR loop	Displays outbound denials of local originated routes.
* unsuppress-map	Displays inbound denials due to an unsuppress map.
* advertise-map	Displays inbound denials due to an advertise map.
* VPN Imported prefix	Displays inbound denials of VPN prefixes.
* Well-known Community	Displays inbound denials of well-known communities.
* SOO loop	Displays inbound denials due to site-of-origin.
* Bestpath from this peer	Displays inbound denials because the best path came from the local router.
* Suppressed due to dampening	Displays inbound denials because the neighbor or link is in a dampening state.
* Bestpath from iBGP peer	Deploys inbound denials because the best path came from an iBGP neighbor.
* Incorrect RIB for CE	Deploys inbound denials due to RIB errors for a customer edge (CE) router.
* BGP distribute-list	Displays inbound denials due to a distribute list.
Number of NLRI...	Number of network layer reachability attributes in updates.
Connections established	Number of times a TCP and BGP connection has been successfully established.

Field	Description
dropped	Number of times that a valid session has failed or been taken down.
Last reset	Time, in hh:mm:ss, since this peering session was last reset. The reason for the reset is displayed on this line.
External BGP neighbor may be...	Indicates that the BGP time to live (TTL) security check is enabled. The maximum number of hops that can separate the local and remote peer is displayed on this line.
Connection state	Connection status of the BGP peer.
unread input bytes	Number of bytes of packets still to be processed.
Connection is ECN Disabled	Explicit congestion notification status (enabled or disabled).
Local host: 10.108.50.1, Local port: 179	IP address of the local BGP speaker. BGP port number 179.
Foreign host: 10.108.50.2, Foreign port: 42698	Neighbor address and BGP destination port number.
Enqueued packets for retransmit:	Packets queued for retransmission by TCP.
Event Timers	TCP event timers. Counters are provided for starts and wakeups (expired timers).
Retrans	Number of times a packet has been retransmitted.
TimeWait	Time waiting for the retransmission timers to expire.
AckHold	Acknowledgment hold timer.
SendWnd	Transmission (send) window.
KeepAlive	Number of keepalive packets.
GiveUp	Number of times a packet is dropped due to no acknowledgment.
PmtuAger	Path MTU discovery timer.
DeadWait	Expiration timer for dead segments.
iss:	Initial packet transmission sequence number.
snduna:	Last transmission sequence number that has not been acknowledged.
sndnxt:	Next packet sequence number to be transmitted.
sndwnd:	TCP window size of the remote neighbor.
irs:	Initial packet receive sequence number.
rcvnxt:	Last receive sequence number that has been locally acknowledged.

show ip bgp neighbors

Field	Description
rcvwnd:	TCP window size of the local host.
delrcvwnd:	Delayed receive window—data the local host has read from the connection, but has not yet subtracted from the receive window the host has advertised to the remote host. The value in this field gradually increases until it is higher than a full-sized packet, at which point it is applied to the rcvwnd field.
SRTT:	A calculated smoothed round-trip timeout.
RTTO:	Round-trip timeout.
RTV:	Variance of the round-trip time.
KRTT:	New round-trip timeout (using the Karn algorithm). This field separately tracks the round-trip time of packets that have been re-sent.
minRTT:	Shortest recorded round-trip timeout (hard-wire value used for calculation).
maxRTT:	Longest recorded round-trip timeout.
ACK hold:	Length of time the local host will delay an acknowledgment to carry (piggyback) additional data.
IP Precedence value:	IP precedence of the BGP packets.
Datagrams	Number of update packets received from a neighbor.
Rcvd:	Number of received packets.
out of order:	Number of packets received out of sequence.
with data	Number of update packets sent with data.
total data bytes	Total amount of data received, in bytes.
Sent	Number of update packets sent.
Second Congestion	Number of update packets with data sent.
Datagrams: Rcvd	Number of update packets received from a neighbor.
retransmit	Number of packets retransmitted.
fastretransmit	Number of duplicate acknowledgments retransmitted for an out of order segment before the retransmission timer expires.
partialack	Number of retransmissions for partial acknowledgments (transmissions before or without subsequent acknowledgments).
Second Congestion	Number of second retransmissions sent due to congestion.

show ip bgp neighbors (4-Byte Autonomous System Numbers)

The following partial example shows output for several external BGP neighbors in autonomous systems with 4-byte autonomous system numbers, 65536 and 65550. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, or a later release.

```
Device# show ip bgp neighbors

BGP neighbor is 192.168.1.2, remote AS 65536, external link
  BGP version 4, remote router ID 0.0.0.0
  BGP state = Idle
  Last read 02:03:38, last write 02:03:38, hold time is 120, keepalive interval is 70
  seconds
    Configured hold time is 120, keepalive interval is 70 seconds
    Minimum holdtime from neighbor is 0 seconds
  .
  .
  .

BGP neighbor is 192.168.3.2, remote AS 65550, external link
  Description: finance
  BGP version 4, remote router ID 0.0.0.0
  BGP state = Idle
  Last read 02:03:48, last write 02:03:48, hold time is 120, keepalive interval is 70
  seconds
    Configured hold time is 120, keepalive interval is 70 seconds
    Minimum holdtime from neighbor is 0 seconds
```

show ip bgp neighbors advertised-routes

The following example displays routes advertised for only the 172.16.232.178 neighbor:

```
Device# show ip bgp neighbors 172.16.232.178 advertised-routes

BGP table version is 27, local router ID is 172.16.232.181
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
Network          Next Hop          Metric LocPrf Weight Path
*>i10.0.0.0      172.16.232.179      0     100      0 ?
*> 10.20.2.0     10.0.0.0          0           32768 i
```

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

Table 138: show ip bgp neighbors advertised-routes Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This is the primary routing table with which the neighbor has been updated. The number increments when the table changes.
local router ID	IP address of the local BGP speaker.

show ip bgp neighbors

Field	Description
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: <ul style="list-style-type: none"> • s—The table entry is suppressed. • d—The table entry is dampened and will not be advertised to BGP neighbors. • h—The table entry does not contain the best path based on historical information. • *—The table entry is valid. • >—The table entry is the best entry to use for that network. • i—The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: <ul style="list-style-type: none"> • i—Entry originated from Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. • e—Entry originated from Exterior Gateway Protocol (EGP). • ?—Origin of the path is not clear. Usually, this is a route that is redistributed into BGP from an IGP.
Network	IP address of a network entity.
Next Hop	IP address of the next system used to forward a packet to the destination network. An entry of 0.0.0.0 indicates that there are non-BGP routes in the path to the destination network.
Metric	If shown, this is the value of the interautonomous system metric. This field is not used frequently.
LocPrf	Local preference value as set with the set local-preference route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

show ip bgp neighbors check-control-plane-failure

The following is sample output from the **show ip bgp neighbors** command entered with the **check-control-plane-failure** option configured:

```
Device# show ip bgp neighbors 10.10.10.1
BGP neighbor is 10.10.10.1, remote AS 10, internal link
Fall over configured for session
BFD is configured. BFD peer is Up. Using BFD to detect fast failover (single-hop) with
c-bit check-control-plane-failure.
```

```
Inherits from template cbit-tps for session parameters
BGP version 4, remote router ID 10.7.7.7
BGP state = Established, up for 00:03:55
Last read 00:00:02, last write 00:00:21, hold time is 180, keepalive interval is 60 seconds

Neighbor sessions:
  1 active, is not multisession capable (disabled)
Neighbor capabilities:
  Route refresh: advertised and received(new)
  Four-octets ASN Capability: advertised and received
  Address family IPv4 Unicast: advertised and received
  Enhanced Refresh Capability: advertised and received
  Multisession Capability:
    Stateful switchover support enabled: NO for session 1
```

show ip bgp neighbors paths

The following is sample output from the **show ip bgp neighbors** command entered with the **paths** keyword:

```
Device# show ip bgp neighbors 172.29.232.178 paths 10
Address      Refcount Metric Path
0x60E577B0          2      40 10 ?
```

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

Table 139: show ip bgp neighbors paths Field Descriptions

Field	Description
Address	Internal address where the path is stored.
RefCount	Number of routes using that path.
Metric	Multi Exit Discriminator (MED) metric for the path. (The name of this metric for BGP versions 2 and 3 is INTER_AS.)
Path	Autonomous system path for that route, followed by the origin code for that route.

show ip bgp neighbors received prefix-filter

The following example shows that a prefix list that filters all routes in the 10.0.0.0 network has been received from the 192.168.20.72 neighbor:

```
Device# show ip bgp neighbors 192.168.20.72 received prefix-filter
Address family:IPv4 Unicast
ip prefix-list 192.168.20.72:1 entries
  seq 5 deny 10.0.0.0/8 le 32
```

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

show ip bgp neighbors**Table 140: show ip bgp neighbors received prefix-filter Field Descriptions**

Field	Description
Address family	Address family mode in which the prefix filter is received.
ip prefix-list	Prefix list sent from the specified neighbor.

show ip bgp neighbors policy

The following sample output shows the policies applied to the neighbor at 192.168.1.2. The output displays both inherited policies and policies configured on the neighbor device. Inherited policies are policies that the neighbor inherits from a peer group or a peer-policy template.

```
Device# show ip bgp neighbors 192.168.1.2 policy
Neighbor: 192.168.1.2, Address-Family: IPv4 Unicast
Locally configured policies:
  route-map ROUTE in
Inherited policies:
  prefix-list NO-MARKETING in
  route-map ROUTE in
    weight 300
  maximum-prefix 10000
```

Cisco IOS Release 12.0(31)S, 12.4(4)T, 12.2(18)SXE, and 12.2(33)SB

The following is sample output from the **show ip bgp neighbors** command that verifies that Bidirectional Forwarding Detection (BFD) is being used to detect fast failover for the BGP neighbor that is a BFD peer:

```
Device# show ip bgp neighbors
BGP neighbor is 172.16.10.2, remote AS 45000, external link
.
.
.
Using BFD to detect fast failover
```

Cisco IOS Release 12.2(33)SRA and 12.4(20)T

The following is sample output from the **show ip bgp neighbors** command that verifies that BGP TCP path maximum transmission unit (MTU) discovery is enabled for the BGP neighbor at 172.16.1.2:

```
Device# show ip bgp neighbors 172.16.1.2
BGP neighbor is 172.16.1.2, remote AS 45000, internal link
  BGP version 4, remote router ID 172.16.1.99
.
.
.
For address family: IPv4 Unicast
  BGP table version 5, neighbor version 5/0
```

```

.
.
.

Address tracking is enabled, the RIB does have a route to 172.16.1.2
Address tracking requires at least a /24 route to the peer
Connections established 3; dropped 2
Last reset 00:00:35, due to Router ID changed
Transport(tcp) path-mtu-discovery is enabled

.

.

SRTT: 146 ms, RTTO: 1283 ms, RTV: 1137 ms, KRTT: 0 ms
minRTT: 8 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: higher precedence, retransmission timeout, nagle, path mtu capable

```

Cisco IOS Release 12.2(33)SXH

The following is sample output from the **show ip bgp neighbors** command that verifies that the neighbor 192.168.3.2 is a member of the peer group group192 and belongs to the subnet range group 192.168.0.0/16, which shows that this BGP neighbor was dynamically created:

```

Device# show ip bgp neighbors 192.168.3.2

BGP neighbor is *192.168.3.2, remote AS 50000, external link
Member of peer-group group192 for session parameters
Belongs to the subnet range group: 192.168.0.0/16
BGP version 4, remote router ID 192.168.3.2
BGP state = Established, up for 00:06:35
Last read 00:00:33, last write 00:00:25, hold time is 180, keepalive intervals
Neighbor capabilities:
  Route refresh: advertised and received(new)
  Address family IPv4 Unicast: advertised and received
Message statistics:
  InQ depth is 0
  OutQ depth is 0

      Sent          Rcvd
Opens:           1            1
Notifications:   0            0
Updates:         0            0
Keepalives:      7            7
Route Refresh:   0            0
Total:           8            8

Default minimum time between advertisement runs is 30 seconds
For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1/0
  Output queue size : 0
  Index 1, Offset 0, Mask 0x2
  1 update-group member
    group192 peer-group member
.
.
.
```

show ip bgp neighbors

Cisco IOS Releases 12.2(33)SRC and 12.2(33)SB

The following is partial output from the **show ip bgp neighbors** command that verifies the status of the BGP graceful restart capability for the external BGP peer at 192.168.3.2. Graceful restart is shown as disabled for this BGP peer.

```
Device# show ip bgp neighbors 192.168.3.2

BGP neighbor is 192.168.3.2, remote AS 50000, external link
  Inherits from template S2 for session parameters
    BGP version 4, remote router ID 192.168.3.2
    BGP state = Established, up for 00:01:41
    Last read 00:00:45, last write 00:00:45, hold time is 180, keepalive intervals
    Neighbor sessions:
      1 active, is multisession capable
    Neighbor capabilities:
      Route refresh: advertised and received(new)
      Address family IPv4 Unicast: advertised and received
      .
      .
      .
      Address tracking is enabled, the RIB does have a route to 192.168.3.2
      Connections established 1; dropped 0
      Last reset never
      Transport(tcp) path-mtu-discovery is enabled
      Graceful-Restart is disabled
      Connection state is ESTAB, I/O status: 1, unread input bytes: 0
```

Cisco IOS Release 15.1(1)S: Example

The following is partial output from the **show ip bgp neighbors** command. For this release, the display includes the Layer 2 VFN address family information if graceful restart or NSF is enabled.

```
Device# show ip bgp neighbors

Load for five secs: 2%/0%; one minute: 0%; five minutes: 0%
Time source is hardware calendar, *21:49:17.034 GMT Wed Sep 22 2010
BGP neighbor is 10.1.1.3, remote AS 2, internal link
  BGP version 4, remote router ID 10.1.1.3
  BGP state = Established, up for 00:14:32
  Last read 00:00:30, last write 00:00:43, hold time is 180, keepalive interval is 60 seconds

  Neighbor sessions:
    1 active, is not multisession capable (disabled)
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Four-octets ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised and received
    Address family L2VPN Vpls: advertised and received
    Graceful Restart Capability: advertised and received
      Remote Restart timer is 120 seconds
      Address families advertised by peer:
        IPv4 Unicast (was not preserved), L2VPN Vpls (was not preserved)
    Multisession Capability:
  Message statistics:
    InQ depth is 0
    OutQ depth is 0
```

```

Sent          Rcvd
Opens:        1          1
Notifications: 0          0
Updates:      4          16
Keepalives:   16         16
Route Refresh: 0          0
Total:        21         33

Default minimum time between advertisement runs is 0 seconds
For address family: IPv4 Unicast
Session: 10.1.1.3
BGP table version 34, neighbor version 34/0
Output queue size : 0
Index 1, Advertise bit 0
1 update-group member
Slow-peer detection is disabled
Slow-peer split-update-group dynamic is disabled
Sent          Rcvd
Prefix activity:  -----
Prefixes Current: 2          11 (Consumes 572 bytes)
Prefixes Total:   4          19
Implicit Withdraw: 2          6
Explicit Withdraw: 0          2
Used as bestpath: n/a        7
Used as multipath: n/a        0
Outbound        Inbound
Local Policy Denied Prefixes:  -----
NEXT_HOP is us:    n/a        1
Bestpath from this peer: 20        n/a
Bestpath from iBGP peer: 8          n/a
Invalid Path:     10         n/a
Total:            38         1

Number of NLIRIs in the update sent: max 2, min 0
Last detected as dynamic slow peer: never
Dynamic slow peer recovered: never
For address family: L2VPN Vpls
Session: 10.1.1.3
BGP table version 8, neighbor version 8/0
Output queue size : 0
Index 1, Advertise bit 0
1 update-group member
Slow-peer detection is disabled
Slow-peer split-update-group dynamic is disabled
Sent          Rcvd
Prefix activity:  -----
Prefixes Current: 1          1 (Consumes 68 bytes)
Prefixes Total:   2          1
Implicit Withdraw: 1          0
Explicit Withdraw: 0          0
Used as bestpath: n/a        1
Used as multipath: n/a        0
Outbound        Inbound
Local Policy Denied Prefixes:  -----
Bestpath from this peer: 4          n/a
Bestpath from iBGP peer: 1          n/a
Invalid Path:     2          n/a
Total:            7          0

Number of NLIRIs in the update sent: max 1, min 0
Last detected as dynamic slow peer: never
Dynamic slow peer recovered: never
Address tracking is enabled, the RIB does have a route to 10.1.1.3
Connections established 1; dropped 0
Last reset never
Transport(tcp) path-mtu-discovery is enabled
Graceful-Restart is enabled, restart-time 120 seconds, stalepath-time 360 seconds

```

show ip bgp neighbors

```

Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Connection is ECN Disabled
Minum incoming TTL 0, Outgoing TTL 255
Local host: 10.1.1.1, Local port: 179
Foreign host: 10.1.1.3, Foreign port: 48485
Connection tableid (VRF): 0
Enqueued packets for retransmit: 0, input: 0 mis-ordered: 0 (0 bytes)
Event Timers (current time is 0xE750C):
    Timer           Starts      Wakeups      Next
Retrans            18          0            0x0
TimeWait           0          0            0x0
AckHold            22          20           0x0
SendWnd            0          0            0x0
KeepAlive          0          0            0x0
GiveUp             0          0            0x0
PmtuAger           0          0            0x0
DeadWait           0          0            0x0
Linger             0          0            0x0
iss: 3196633674  snduna: 3196634254  sndnxt: 3196634254      sndwnd: 15805
irs: 1633793063  rcvnx: 1633794411  rcvwnd: 15037  delrcvwnd: 1347
SRTT: 273 ms, RTTO: 490 ms, RTV: 217 ms, KRTT: 0 ms
minRTT: 2 ms, maxRTT: 300 ms, ACK hold: 200 ms
Status Flags: passive open, gen tcbs
Option Flags: nagle, path mtu capable
Datagrams (max data segment is 1436 bytes):
Rcvd: 42 (out of order: 0), with data: 24, total data bytes: 1347
Sent: 40 (retransmit: 0 fastretransmit: 0), with data: 19, total data bytes: 579

```

BGP Attribute Filter and Enhanced Attribute Error Handling

The following is sample output from the **show ip bgp neighbors** command that indicates the discard attribute values and treat-as-withdraw attribute values configured. It also provides a count of received Updates matching a treat-as-withdraw attribute, a count of received Updates matching a discard attribute, and a count of received malformed Updates that are treat-as-withdraw.

```

Device# show ip bgp vpng4 all neighbors 10.0.103.1

BGP neighbor is 10.0.103.1, remote AS 100, internal link
  Path-attribute treat-as-withdraw inbound
  Path-attribute treat-as-withdraw value 128
  Path-attribute treat-as-withdraw 128 in: count 2
  Path-attribute discard 128 inbound
  Path-attribute discard 128 in: count 2

      Outbound      Inbound
  Local Policy Denied Prefixes:  -----  -----
      MALFORM treat as withdraw:        0          1
      Total:                      0          1

```

BGP Additional Paths

The following output indicates that the neighbor is capable of advertising additional paths and sending additional paths it receives. It is also capable of receiving additional paths and advertised paths.

```

Device# show ip bgp neighbors 10.108.50.2

BGP neighbor is 10.108.50.2, remote AS 1, internal link
  BGP version 4, remote router ID 192.168.252.252

```

```
BGP state = Established, up for 00:24:25
Last read 00:00:24, last write 00:00:24, hold time is 180, keepalive interval is 60 seconds

Neighbor capabilities:
  Additional paths Send: advertised and received
  Additional paths Receive: advertised and received
  Route refresh: advertised and received(old & new)
  Graceful Restart Capabilty: advertised and received
  Address family IPv4 Unicast: advertised and received
```

BGP—Multiple Cluster IDs

In the following output, the cluster ID of the neighbor is displayed. (The vertical bar and letter “i” for “include” cause the device to display only lines that include the user’s input after the “i”, in this case, “cluster-id.”) The cluster ID displayed is the one directly configured through a neighbor or a template.

```
Device# show ip bgp neighbors 192.168.2.2 | i cluster-id
```

```
Configured with the cluster-id 192.168.15.6
```

Related Commands	Command	Description
	bgp asnotation dot	Changes the default display and the regular expression match format of BGP 4-byte autonomous system numbers from asplain (decimal values) to dot notation.
	bgp enhanced-error	Restores the default behavior of treating Update messages that have a malformed attribute as withdrawn, or includes iBGP peers in the Enhanced Attribute Error Handling feature.
	neighbor path-attribute discard	Configures the device to discard unwanted Update messages from the specified neighbor that contain a specified path attribute.
	neighbor path-attribute treat-as-withdraw	Configures the device to withdraw from the specified neighbor unwanted Update messages that contain a specified attribute.
	neighbor send-label	Enables a BGP router to send MPLS labels with BGP routes to a neighboring BGP router.
	neighbor send-label explicit-null	Enables a BGP router to send MPLS labels with explicit-null information for a CSC-CE router and BGP routes to a neighboring CSC-PE router.
	router bgp	Configures the BGP routing process.

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}]
```

show ip eigrp interfaces

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 Everest 16.6.1	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 141: show ip eigrp interfaces Field Descriptions

Field	Description
Interface	Interface on which EIGRP is configured.
Peers	Number of directly connected EIGRP neighbors.
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 .

show ip eigrp neighbors

Field	Description
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 <i>vrf-name</i>	(Optional) Displays information about the specified VPN Routing and Forwarding (VRF) instance.
<i>autonomous-system-number</i>	(Optional) Autonomous-system-number-specific output is displayed.
static	(Optional) Displays static neighbors.
detail	(Optional) Displays detailed neighbor information.
<i>interface-type</i> <i>interface-number</i>	(Optional) Interface-specific output is displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Everest 16.6.1	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 (sec)	Uptime (sec)	SRTT (ms)	RTO 5000	Q 0	Seq 5
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 142: 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.
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 (sec)	Uptime (sec)	SRTT (ms)	RTO 1600	Q 5000	Seq 0
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.

show ip eigrp topology

Table 143: 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.
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 | frr | pending | secondary-paths | summary | zero-successors{}]

Syntax Description

<i>network</i>	(Optional) Network address.
<i>mask</i>	(Optional) Network mask.
<i>prefix</i>	(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 entries in the EIGRP topology table (including nonfeasible-successor sources).
detail-links	(Optional) Displays all topology entries with additional details.
frr	(Optional) Displays the list of configured loop-free alternates in the EIGRP topology table.
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.
secondary-paths	(Optional) Displays secondary paths in the topology.
summary	(Optional) Displays a summary of the EIGRP topology table.
zero-successors	(Optional) Displays 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 Everest 16.6.1	This command was introduced.
	Cisco IOS XE Amsterdam 17.2.1	The frr keyword 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 paths, whether feasible or not, and the **detail-links** keyword displays additional details about these paths.

Use this command to display information about EIGRP named and EIGRP autonomous system configurations. This command displays the same information as the **show eigrp address-family topology** command. We recommend using the **show eigrp address-family topology** command.

Examples The following is sample output from the **show ip eigrp topology** command:

```
Device# show ip eigrp topology

EIGRP-IPv4 Topology Table for AS(1)/ID(10.0.0.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status, s - sia status
P 10.0.0.0/8, 1 successors, FD is 409600
      via 192.0.2.1 (409600/128256), Ethernet0/0
P 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
```

show ip eigrp topology

```
P 10.0.1.0/24, 1 successors, FD is 281600
    via Connected, Ethernet0/0
```

The following sample output from the **show ip eigrp topology prefix** command displays detailed information about a single prefix. The prefix shown is an EIGRP internal route.

```
Device# show ip eigrp topology 10.0.0.0/8
```

```
EIGRP-IPv4 VR(vr1) Topology Entry for AS(1)/ID(10.1.1.2) for 10.0.0.0/8
State is Passive, Query origin flag is 1, 1 Successor(s), FD is 82329600, RIB is 643200
Descriptor Blocks:
10.1.1.1 (Ethernet2/0), from 10.1.1.1, Send flag is 0x0
    Composite metric is (82329600/163840), route is Internal
    Vector metric:
        Minimum bandwidth is 16000 Kbit
        Total delay is 631250000 picoseconds
        Reliability is 255/255
        Load is %55
        Minimum MTU is 1500
        Hop count is 1
        Originating router is 10.1.1.1
```

The following sample output from the **show ip eigrp topology prefix** command displays detailed information about a single prefix. The prefix shown is an EIGRP external route.

```
Device# show ip eigrp topology 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 %55
        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 sample output from the **show ip eigrp topology prefix** command displays Equal Cost Multipath (ECMP) mode information when the **no ip next-hop-self** command is configured without the **no-ecmp-mode** keyword in an EIGRP topology. The ECMP mode provides information about the path that is being advertised. If there is more than one successor, the top most path will be advertised as the default path over all interfaces, and “ECMP Mode: Advertise by default” will be displayed in the output. If any path other than the default path is advertised, “ECMP Mode: Advertise out <Interface name>” will be displayed.

The topology table displays entries of routes for a particular prefix. The routes are sorted based on metric, next-hop, and infosource. In a Dynamic Multipoint VPN (DMVPN) scenario, routes with same metric and next-hop are sorted based on infosource. The top route in the ECMP is always advertised.

```
Device# show ip eigrp topology 192.168.10.0/24
```

```
EIGRP-IPv4 Topology Entry for AS(1)/ID(10.10.100.100) for 192.168.10.0/24
```

```

State is Passive, Query origin flag is 1, 2 Successor(s), FD is 284160
Descriptor Blocks:
 10.100.1.0 (Tunnel0), from 10.100.0.1, Send flag is 0x0
    Composite metric is (284160/281600), route is Internal
    Vector metric:
      Minimum bandwidth is 10000 Kbit
      Total delay is 1100 microseconds
      Reliability is 255/255
      Load is 255
      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 255
      Minimum MTU is 1400
      Hop count is 1
      Originating router is 10.10.2.2
ECMP Mode: Advertise out Tunnel1

```

The following sample output from the **show ip eigrp topology all-links** command displays all paths, even those that are not feasible:

```

Device# show ip eigrp topology all-links

EIGRP-IPv4 Topology Table for AS(1)/ID(10.0.0.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status
P 172.16.1.0/24, 1 successors, FD is 409600, serno 14
  via 10.10.1.2 (409600/128256), Ethernet0/0
  via 10.1.4.3 (2586111744/2585599744), Serial13/0, serno 18

```

The following sample output from the **show ip eigrp topology detail-links** command displays additional details about routes:

```

Device# show ip eigrp topology detail-links

EIGRP-IPv4 Topology Table for AS(1)/ID(10.0.0.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status
P 10.0.0.0/8, 1 successors, FD is 409600, serno 6
  via 10.10.1.2 (409600/128256), Ethernet0/0
P 172.16.1.0/24, 1 successors, FD is 409600, serno 14
  via 10.10.1.2 (409600/128256), Ethernet0/0
P 10.0.0.0/8, 1 successors, FD is 281600, serno 3
  via Summary (281600/0), Null0
P 10.1.1.0/24, 1 successors, FD is 281600, serno 1
  via Connected, Ethernet0/0

```

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

show ip eigrp topology

Table 144: show ip eigrp topology Field Descriptions

Field	Description
Codes	<p>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> <ul style="list-style-type: none"> • 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. The feasible distance is the best metric to reach the destination or the best metric that was known when the route became active. This value is used in the feasibility condition check. If the reported distance of the device is less than the feasible distance, the feasibility condition is met and that route becomes a feasible successor. After the software determines that it has a feasible successor, the software need not send a query for that destination.
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	<table border="1"> <tr> <td>vrf vrf-name</td><td>(Optional) Displays information about the specified VRF.</td></tr> <tr> <td>vrf *</td><td>(Optional) Displays information about all VRFs.</td></tr> <tr> <td><i>autonomous-system-number</i></td><td>(Optional) Autonomous system number.</td></tr> </table>	vrf vrf-name	(Optional) Displays information about the specified VRF.	vrf *	(Optional) Displays information about all VRFs.	<i>autonomous-system-number</i>	(Optional) Autonomous system number.
vrf vrf-name	(Optional) Displays information about the specified VRF.						
vrf *	(Optional) Displays information about all VRFs.						
<i>autonomous-system-number</i>	(Optional) Autonomous system number.						

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

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	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 145: 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.

show ip ospf

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

<i>process-id</i>	(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 Everest 16.6.1	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 msec
Retransmission pacing timer 100 msec
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 msec
Minimum hold time between two consecutive SPFs 10000 msec
Maximum wait time between two consecutive SPFs 10000 msec
Incremental-SPF disabled
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msec
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msec
Retransmission pacing timer 66 msec
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

```

```
show ip ospf
```

```

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 146: 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.
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 msec
Minimum hold time between two consecutive SPFs 10000 msec
Maximum wait time between two consecutive SPFs 10000 msec
Incremental-SPF disabled
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msec
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msec
Retransmission pacing timer 66 msec
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 147: 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).

show ip ospf

Field	Description
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 148: 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.

Field	Description
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 timersthottlespf command.
Minimum hold time between two consecutive SPFs	Minimum hold time (in milliseconds) between two consecutive SPF calculations for SPF throttling. Configured with the timersthottlespf command.
Maximum wait time between two consecutive SPFs	Maximum wait time (in milliseconds) between two consecutive SPF calculations for SPF throttling. Configured with the timersthottlespf 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 msec
  Minimum hold time between two consecutive SPFs 10000 msec
  Maximum wait time between two consecutive SPFs 10000 msec
  Incremental-SPF disabled
  Initial LSA throttle delay 100 msec
  Minimum hold time for LSA throttle 10000 msec

  Maximum wait time for LSA throttle 45000 msec
  Minimum LSA arrival 1000 msec
  LSA group pacing timer 240 secs
  Interface flood pacing timer 33 msec
  Retransmission pacing timer 66 msec
  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

```

show ip ospf

```
Number of DoNotAge LSA 0
Flood list length 0
```

The following is sample **show ip ospf** command. In this example, the user had configured the **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 msec
Minimum hold time between two consecutive SPFs 10000 msec
Maximum wait time between two consecutive SPFs 10000 msec
```

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

Table 149: 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 **show ip ospf** command. In this example, the user had configured LSA throttling, and those lines of output are displayed in bold.

```
Device#show ip ospf 1
Routing Process "ospf 4" with ID 10.10.24.4
  Supports only single TOS(TOS0) routes
  Supports opaque LSA
  Supports Link-local Signaling (LLS)
  Initial SPF schedule delay 5000 msec
  Minimum hold time between two consecutive SPFs 10000 msec
  Maximum wait time between two consecutive SPFs 10000 msec
  Incremental-SPF disabled
Initial LSA throttle delay 100 msec
Minimum hold time for LSA throttle 10000 msec
Maximum wait time for LSA throttle 45000 msec
  Minimum LSA arrival 1000 msec
  LSA group pacing timer 240 secs
  Interface flood pacing timer 33 msec
  Retransmission pacing timer 66 msec
  Number of external LSA 0. Checksum Sum 0x0
  Number of opaque AS LSA 0. Checksum Sum 0x0
  Number of DCbitless external and opaque AS LSA 0
  Number of DoNotAge external and opaque AS LSA 0
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  External flood list length 0
    Area 24
      Number of interfaces in this area is 2
      Area has no authentication
      SPF algorithm last executed 04:28:18.396 ago
      SPF algorithm executed 8 times
      Area ranges are
      Number of LSA 4. Checksum Sum 0x23EB9
      Number of opaque link LSA 0. Checksum Sum 0x0
      Number of DCbitless LSA 0
      Number of indication LSA 0
      Number of DoNotAge LSA 0
      Flood list length 0
```

show ip ospf border-routers

To display the internal Open Shortest Path First (OSPF) routing table entries to an Area Border Router (ABR) and Autonomous System Boundary Router (ASBR), use the **show ip ospf border-routers** command in privileged EXEC mode.

show ip ospf border-routers

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

Command Modes	Privileged EXEC
----------------------	-----------------

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

show ip ospf database

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 150: 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-originated]
[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-originated] [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-originated] [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-originated] [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	
<i>process-id</i>	(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.
<i>area-id</i>	(Optional) Area number associated with the OSPF address range defined in the network router configuration command used to define the particular area.
adv-router [<i>ip-address</i>]	(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).
<i>link-state-id</i>	(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 <i>link-state-id</i> 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.

show ip ospf database

Command Modes EXEC

Command History	Release	Modification
Cisco IOS XE Everest 16.6.1		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 151: 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 152: show ip ospf database asbr-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.
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 **show ip ospf database** command with the **external** keyword:

```
Device#show ip ospf database external
OSPF Router with id(192.168.239.66) (Autonomous system 300)
          Displaying AS External Link States
LS age: 280
Options: (No TOS-capability)
LS Type: AS External Link
Link State ID: 10.105.0.0 (External Network Number)
Advertising Router: 172.16.70.6
LS Seq Number: 80000AFD
Checksum: 0xC3A
Length: 36
Network Mask: 255.255.0.0
          Metric Type: 2 (Larger than any link state path)
```

show ip ospf database

```
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 153: 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).
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 **show ip ospf database** command with the **network** keyword:

```
Device#show ip ospf database network
OSPF Router with id(192.168.239.66) (Process ID 300)
          Displaying Net Link States(Area 0.0.0.0)
LS age: 1367
Options: (No TOS-capability)
LS Type: Network Links
Link State ID: 172.16.1.3 (address of Designated Router)
Advertising Router: 192.168.239.66
LS Seq Number: 800000E7
Checksum: 0x1229
```

```

Length: 52
Network Mask: 255.255.255.0
Attached Router: 192.168.239.66
Attached Router: 172.16.241.5
Attached Router: 172.16.1.1
Attached Router: 172.16.54.5
Attached Router: 172.16.1.5

```

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

Table 154: show ip ospf database network Field Descriptions

Field	Description
OSPF Router with id	Router ID number.
Process ID 300	OSPF process ID.
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

```

show ip ospf database

```
Number of TOS metrics: 0
TOS 0 Metrics: 2
```

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

Table 155: 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.
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 **show ip ospf database** command with the **summary** keyword:

```
Device#show ip ospf database summary
      OSPF Router with id(192.168.239.66) (Process ID 300)
      Displaying Summary Net Link States(Area 0.0.0.0)
      LS age: 1401
      Options: (No TOS-capability)
      LS Type: Summary Links(Network)
      Link State ID: 172.16.240.0 (summary Network Number)
      Advertising Router: 172.16.241.5
      LS Seq Number: 80000072
      Checksum: 0x84FF
      Length: 28
      Network Mask: 255.255.255.0    TOS: 0    Metric: 1
```

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

Table 156: 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.
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 **show ip ospf database** 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
```

show ip ospf database

Opaque AS	0	0	0
Total	203	0	0

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

Table 157: 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.
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.

Field	Description
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	<i>process-id</i>	(Optional) Process ID number. If this argument is included, only information for the specified routing process is included. The range is 1 to 65535.
	<i>type</i>	(Optional) Interface type. If the <i>type</i> argument is included, only information for the specified interface type is included.
	<i>number</i>	(Optional) Interface number. If the <i>number</i> 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 Everest 16.6.1	This command was introduced.

Examples

The following is sample output from the **show ip ospf interface** command when Ethernet interface 0/0 is specified:

show ip ospf interface

```
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 158: 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.

show ip ospf neighbor

Field	Description
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 **show ip ospf neighbor** command in privileged EXEC mode.

show ip ospf neighbor [interface-type interface-number] [neighbor-id] [detail] [summary] [per-instance]

Syntax Description	<table border="1"> <tr> <td><i>interface-type interface-number</i></td><td>(Optional) Type and number associated with a specific OSPF interface.</td></tr> <tr> <td><i>neighbor-id</i></td><td>(Optional) Neighbor hostname or IP address in A.B.C.D format.</td></tr> <tr> <td>detail</td><td>(Optional) Displays all neighbors given in detail (lists all neighbors).</td></tr> <tr> <td>summary</td><td>(Optional) Displays total number summary of all neighbors.</td></tr> <tr> <td>per-instance</td><td>(Optional) Displays total number of neighbors in each neighbor state. The output is printed for each configured OSPF instance separately.</td></tr> </table>	<i>interface-type interface-number</i>	(Optional) Type and number associated with a specific OSPF interface.	<i>neighbor-id</i>	(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.
<i>interface-type interface-number</i>	(Optional) Type and number associated with a specific OSPF interface.										
<i>neighbor-id</i>	(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 Everest 16.6.1	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 159: show ip ospf neighbor detail Field Descriptions

Field	Description
Neighbor	Neighbor router ID.
interface address	IP address of the interface.

show ip ospf neighbor

Field	Description
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.
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
```

```
show ip ospf neighbor
```

```
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 160: 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 the master, 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 master which is explicitly acknowledged by slave. Routers also send link-state request packets and link-state update packets (which contain the entire LSA) in this state. The contents of the DBD received are compared to the information contained in the routers link-state database to check if new or more current link-state information is available with the neighbor.

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 Everest 16.6.1	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.

summary-address (OSPF)**Table 161: 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 [not-advertise] [tag tag] [nssa-only]
no summary-address [not-advertise] [tag tag] [nssa-only]
```

Syntax Description	<i>ip-address</i>	Summary address designated for a range of addresses.
	<i>mask</i>	IP subnet mask used for the summary route.
	<i>prefix</i>	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 Everest 16.6.1	This command was introduced.

Usage Guidelines	<p>Routes learned from other routing protocols can be summarized. The metric used to advertise the summary is the lowest metric of all the more specific routes. This command helps reduce the size of the routing table.</p> <p>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.</p> <p>OSPF does not support the summary-address 0.0.0.0 0.0.0.0 command.</p>
------------------	--

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	<i>spf-start</i>	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.
	<i>spf-hold</i>	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.
	<i>spf-max-wait</i>	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.
-----------------	----------------------------

timers throttle spf

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 Everest 16.6.1	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

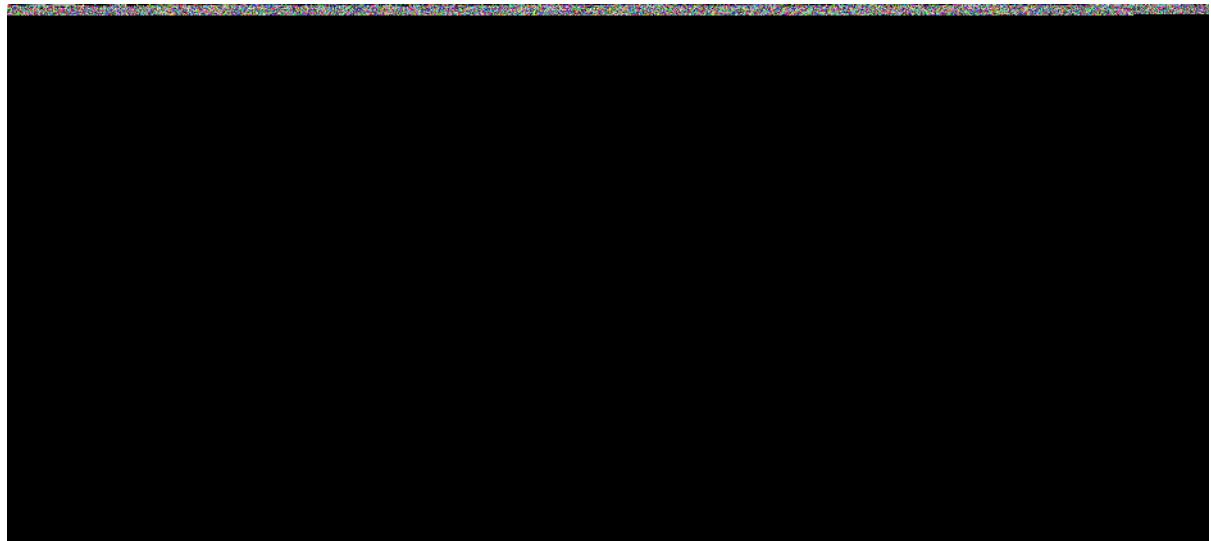
The following example shows how to configure a router with the delay, hold, and maximum interval values for the **timers throttle spf** command set at 5, 1000, and 90,000 milliseconds, respectively.

```
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 0
```

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 **XII**

Security

- [Security, on page 913](#)

CHAPTER 20

Security

- aaa accounting, on page 915
- aaa accounting dot1x, on page 918
- aaa accounting identity, on page 919
- aaa authentication dot1x, on page 920
- aaa new-model, on page 921
- authentication host-mode, on page 922
- authentication mac-move permit, on page 924
- authentication priority, on page 924
- authentication violation, on page 927
- cisp enable, on page 928
- clear errdisable interface vlan, on page 929
- clear mac address-table, on page 930
- confidentiality-offset, on page 931
- cts manual, on page 932
- cts role-based enforcement, on page 933
- cts role-based l2-vrf, on page 934
- cts role-based monitor, on page 936
- cts role-based permissions, on page 937
- delay-protection, on page 938
- deny (MAC access-list configuration), on page 939
- device-role (IPv6 snooping), on page 942
- device-role (IPv6 nd inspection), on page 942
- device-tracking policy, on page 943
- dot1x critical (global configuration), on page 944
- dot1x pae, on page 945
- dot1x supplicant controlled transient, on page 946
- dot1x supplicant force-multicast, on page 946
- dot1x test eapol-capable, on page 947
- dot1x test timeout, on page 948
- dot1x timeout, on page 949
- dtls, on page 951
- epm access-control open, on page 952
- include-icv-indicator, on page 953

- ip access-list role-based, on page 954
- ip admission, on page 955
- ip admission name, on page 955
- ip dhcp snooping database, on page 957
- ip dhcp snooping information option format remote-id, on page 959
- ip dhcp snooping verify no-relay-agent-address, on page 959
- ip http access-class, on page 960
- ip radius source-interface, on page 961
- ip source binding, on page 963
- ip verify source, on page 963
- ipv6 access-list, on page 964
- ipv6 snooping policy, on page 966
- key chain macsec, on page 967
- key-server, on page 968
- limit address-count, on page 969
- mab request format attribute 32, on page 970
- macsec-cipher-suite, on page 971
- macsec network-link, on page 972
- match (access-map configuration), on page 973
- mka pre-shared-key, on page 974
- mka suppress syslogs sak-rekey, on page 974
- authentication logging verbose, on page 975
- dot1x logging verbose, on page 976
- mab logging verbose, on page 977
- permit (MAC access-list configuration), on page 977
- propagate sgt (cts manual), on page 980
- protocol (IPv6 snooping), on page 982
- radius server, on page 982
- sak-rekey, on page 984
- sap mode-list (cts manual), on page 985
- security level (IPv6 snooping), on page 987
- send-secure-announcements, on page 987
- server-private (RADIUS), on page 988
- show aaa clients, on page 990
- show aaa command handler, on page 991
- **show aaa local**, on page 991
- show aaa servers, on page 992
- show aaa sessions, on page 993
- show authentication brief, on page 994
- show authentication sessions, on page 996
- show cts interface, on page 998
- show cts role-based permissions, on page 1000
- show cisp, on page 1001
- show dot1x, on page 1003
- show eap pac peer, on page 1004
- show ip dhcp snooping statistics, on page 1004

- show radius server-group, on page 1007
- show vlan access-map, on page 1008
- show vlan filter, on page 1009
- show vlan group, on page 1009
- switchport port-security aging, on page 1010
- switchport port-security mac-address, on page 1011
- switchport port-security maximum, on page 1013
- switchport port-security violation, on page 1014
- tacacs server, on page 1016
- tracking (IPv6 snooping), on page 1017
- trusted-port, on page 1018
- vlan access-map, on page 1019
- vlan dot1Q tag native, on page 1021
- vlan filter, on page 1021
- vlan group, on page 1022

aaa accounting

To enable authentication, authorization, and accounting (AAA) accounting of requested services for billing or security purposes when you use RADIUS or TACACS+, use the **aaa accounting** command in global configuration mode. To disable AAA accounting, use the **no** form of this command.

```
aaa accounting {auth-proxy | system | network | exec | connections | commands level}
{default | list-name} {start-stop | stop-only | none} [broadcast] group group-name
no aaa accounting {auth-proxy | system | network | exec | connections | commands level}
{default | list-name} {start-stop | stop-only | none} [broadcast] group group-name
```

Syntax Description	
auth-proxy	Provides information about all authenticated-proxy user events.
system	Performs accounting for all system-level events not associated with users, such as reloads.
network	Runs accounting for all network-related service requests.
exec	Runs accounting for EXEC shell session. This keyword might return user profile information such as what is generated by the autocommand command.
connection	Provides information about all outbound connections made from the network access server.
commands level	Runs accounting for all commands at the specified privilege level. Valid privilege level entries are integers from 0 through 15.
default	Uses the listed accounting methods that follow this argument as the default list of methods for accounting services.
<i>list-name</i>	Character string used to name the list of at least one of the accounting methods described in

start-stop	Sends a "start" accounting notice at the beginning of a process and a "stop" accounting notice at the end of a process. The "start" accounting record is sent in the background. The requested user process begins regardless of whether the "start" accounting notice was received by the accounting server.				
stop-only	Sends a "stop" accounting notice at the end of the requested user process.				
none	Disables accounting services on this line or interface.				
broadcast	(Optional) Enables sending accounting records to multiple AAA servers. Simultaneously sends accounting records to the first server in each group. If the first server is unavailable, fail over occurs using the backup servers defined within that group.				
<i>group groupname</i>	At least one of the keywords described in Table 162: AAA accounting Methods, on page 916				
Command Default	AAA accounting is disabled.				
Command Modes	Global configuration				
Command History	<table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; width: 40%;">Release</th> <th style="text-align: left;">Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	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 162: AAA accounting Methods

Keyword	Description
group radius	Uses the list of all RADIUS servers for authentication as defined by the aaa group server radius command.
group tacacs+	Uses the list of all TACACS+ servers for authentication as defined by the aaa group server tacacs+ command.
group group-name	Uses a subset of RADIUS or TACACS+ servers for accounting as defined by the server group group-name.

In [Table 162: AAA accounting Methods, on page 916](#), the **group radius** and **group tacacs+** methods refer to a set of previously defined RADIUS or TACACS+ servers. Use the **radius server** and **tacacs server** commands to configure the host servers. Use the **aaa group server radius** and **aaa group server tacacs+** commands to create a named group of servers.

Cisco IOS software supports the following two methods of accounting:

- RADIUS—The network access server reports user activity to the RADIUS security server in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server.

- TACACS+—The network access server reports user activity to the TACACS+ security server in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server.

Method lists for accounting define the way accounting will be performed. Named accounting method lists enable you to designate a particular security protocol to be used on specific lines or interfaces for particular types of accounting services. Create a list by entering the *list-name* and the *method*, where *list-name* is any character string used to name this list (excluding the names of methods, such as radius or tacacs+) and *method* identifies the methods to be tried in sequence as given.

If the **aaa accounting** command for a particular accounting type is issued without a named method list specified, the default method list is automatically applied to all interfaces or lines (where this accounting type applies) except those that have a named method list explicitly defined. (A defined method list overrides the default method list.) If no default method list is defined, then no accounting takes place.

**Note**

System accounting does not use named accounting lists; you can only define the default list for system accounting.

For minimal accounting, include the **stop-only** keyword to send a stop record accounting notice at the end of the requested user process. For more accounting, you can include the **start-stop** keyword, so that RADIUS or TACACS+ sends a start accounting notice at the beginning of the requested process and a stop accounting notice at the end of the process. Accounting is stored only on the RADIUS or TACACS+ server. The **none** keyword disables accounting services for the specified line or interface.

When AAA accounting is activated, the network access server monitors either RADIUS accounting attributes or TACACS+ AV pairs pertinent to the connection, depending on the security method you have implemented. The network access server reports these attributes as accounting records, which are then stored in an accounting log on the security server. For a list of supported RADIUS accounting attributes, refer to the appendix RADIUS Attributes in the *Cisco IOS Security Configuration Guide*. For a list of supported TACACS+ accounting AV pairs, refer to the appendix TACACS+ Attribute-Value Pairs in the *Cisco IOS Security Configuration Guide*.

**Note**

This command cannot be used with TACACS or extended TACACS.

This example defines a default commands accounting method list, where accounting services are provided by a TACACS+ security server, set for privilege level 15 commands with a stop-only restriction:

```
Device(config)# aaa accounting commands 15 default stop-only group TACACS+
```

This example defines a default auth-proxy accounting method list, where accounting services are provided by a TACACS+ security server with a stop-only restriction. The **aaa accounting** command activates authentication proxy accounting.

```
Device(config)# aaa new model
Device(config)# aaa authentication login default group TACACS+
Device(config)# aaa authorization auth-proxy default group TACACS+
Device(config)# aaa accounting auth-proxy default start-stop group TACACS+
```

aaa accounting dot1x

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	<p>name Name of a server group. This is optional when you enter it after the broadcast group and group keywords.</p> <p>default Specifies the accounting methods that follow as the default list for accounting services.</p> <p>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.</p> <p>broadcast Enables accounting records to be sent to multiple AAA servers and sends accounting records to the first server in each group. If the first server is unavailable, the switch uses the list of backup servers to identify the first server.</p> <p>group Specifies the server group to be used for accounting services. These are valid server group names: <ul style="list-style-type: none"> • name — Name of a server group. • radius — Lists of all RADIUS hosts. • tacacs+ — Lists of all TACACS+ hosts. The group keyword is optional when you enter it after the broadcast group and group keywords. You can enter more than optional group keyword. </p> <p>radius (Optional) Enables RADIUS accounting.</p> <p>tacacs+ (Optional) Enables TACACS+ accounting.</p>				
Command Default	AAA accounting is disabled.				
Command Modes	Global configuration				
Command History	<table border="0"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				

Usage Guidelines

This command requires access to a RADIUS server.

We recommend that you enter the **dot1x reauthentication** interface configuration command before configuring IEEE 802.1x RADIUS accounting on an interface.

This example shows how to configure IEEE 802.1x accounting:

```
Device(config)# aaa new-model
Device(config)# aaa accounting dot1x default start-stop group radius
```

aaa accounting identity

To enable authentication, authorization, and accounting (AAA) 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	<p>name Name of a server group. This is optional when you enter it after the broadcast group and group keywords.</p> <p>default Uses the accounting methods that follow as the default list for accounting services.</p> <p>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.</p> <p>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.</p> <p>group Specifies the server group to be used for accounting services. These are valid server group names: <ul style="list-style-type: none"> • name — Name of a server group. • radius — Lists of all RADIUS hosts. • tacacs+ — Lists of all TACACS+ hosts. The group keyword is optional when you enter it after the broadcast group and group keywords. You can enter more than one optional group keyword. </p> <p>radius (Optional) Enables RADIUS authorization.</p> <p>tacacs+ (Optional) Enables TACACS+ accounting.</p>
--------------------	---

aaa authentication dot1x

Command Default	AAA accounting is disabled.				
Command Modes	Global configuration				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				

Usage Guidelines To enable AAA accounting identity, you need to enable policy mode. To enable policy mode, enter the **authentication display new-style** command in privileged EXEC mode.

This example shows how to configure IEEE 802.1x accounting identity:

```
Device# authentication display new-style
```

Please note that while you can revert to legacy style configuration at any time unless you have explicitly entered new-style configuration, the following caveats should be carefully read and understood.

- (1) If you save the config in this mode, it will be written to NVRAM in NEW-style config, and if you subsequently reload the router without reverting to legacy config and saving that, you will no longer be able to revert.
- (2) In this and legacy mode, Webauth is not IPv6-capable. It will only become IPv6-capable once you have entered new-style config manually, or have reloaded with config saved in 'authentication display new' mode.

```
Device# configure terminal
Device(config)# aaa accounting identity default start-stop group radius
```

aaa authentication dot1x

To specify the authentication, authorization, and accounting (AAA) method to use on ports complying with the IEEE 802.1x authentication, use the **aaa authentication dot1x** command in global configuration mode on a standalone switch. To disable authentication, use the **no** form of this command.

```
aaa authentication dot1x {default} method1
no aaa authentication dot1x {default} method1
```

Syntax Description	<p>default The default method when a user logs in. Use the listed authentication method that follows this argument.</p> <p>method1 Specifies the server authentication. Enter the group radius keywords to use the list of all RADIUS servers for authentication.</p> <p>Note Though other keywords are visible in the command-line help strings, only the default and group radius keywords are supported.</p>
---------------------------	---

Command Default	No authentication is performed.				
Command Modes	Global configuration				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				
Usage Guidelines	<p>The method argument identifies the method that the authentication algorithm tries in the specified sequence to validate the password provided by the client. The only method that is IEEE 802.1x-compliant is the group radius method, in which the client data is validated against a RADIUS authentication server.</p> <p>If you specify group radius, you must configure the RADIUS server by entering the radius-server host global configuration command.</p> <p>Use the show running-config privileged EXEC command to display the configured lists of authentication methods.</p> <p>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.</p> <pre>Device(config)# aaa new-model Device(config)# aaa authentication dot1x default group radius</pre>				

aaa new-model

To enable the authentication, authorization, and accounting (AAA) access control model, issue the **aaa new-model** command in global configuration mode. To disable the AAA access control model, use the **no** form of this command.

```
aaa new-model
no aaa new-model
```

Syntax Description	This command has no arguments or keywords.				
Command Default	AAA is not enabled.				
Command Modes	Global configuration (config)				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	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.

authentication host-mode

Note We do not recommend removing the **aaa new-model** command.

The following example shows this restriction:

```
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
!
```

Examples

The following example initializes AAA:

```
Device(config)# aaa new-model
Device(config)#

```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.
aaa authentication arap	Enables an AAA authentication method for ARAP using TACACS+.
aaa authentication enable default	Enables AAA authentication to determine if a user can access the privileged command level.
aaa authentication login	Sets AAA authentication at login.
aaa authentication ppp	Specifies one or more AAA authentication method for use on serial interfaces running PPP.
aaa authorization	Sets parameters that restrict user access to a network.

authentication host-mode

To set the authorization manager mode on a port, use the **authentication host-mode** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

```
authentication host-mode { multi-auth | multi-domain | multi-host | single-host }
no authentication host-mode
```

Syntax Description	multi-auth	Enables multiple-authorization mode (multi-auth mode) on the port.
	multi-domain	Enables multiple-domain mode on the port.
	multi-host	Enables multiple-host mode on the port.
	single-host	Enables single-host mode on the port.

Command Default Single host mode is enabled.

Command Modes Interface configuration

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines Single-host mode should be configured if only one data host is connected. Do not connect a voice device to authenticate on a single-host port. Voice device authorization fails if no voice VLAN is configured on the port.

Multi-domain mode should be configured if data host is connected through an IP phone to the port. Multi-domain mode should be configured if the voice device needs to be authenticated.

Multi-auth mode should be configured to allow devices behind a hub to obtain secured port access through individual authentication. Only one voice device can be authenticated in this mode if a voice VLAN is configured.

Multi-host mode also offers port access for multiple hosts behind a hub, but multi-host mode gives unrestricted port access to the devices after the first user gets authenticated.

This example shows how to enable multi-auth mode on a port:

```
Device(config-if)# authentication host-mode multi-auth
```

This example shows how to enable multi-domain mode on a port:

```
Device(config-if)# authentication host-mode multi-domain
```

This example shows how to enable multi-host mode on a port:

```
Device(config-if)# authentication host-mode multi-host
```

This example shows how to enable single-host mode on a port:

```
Device(config-if)# authentication host-mode single-host
```

You can verify your settings by entering the **show authentication sessions interface *interface details* privileged EXEC** command.

authentication mac-move permit

authentication mac-move permit

To enable MAC move on a device, use the **authentication mac-move permit** command in global configuration mode. To disable MAC move, use the **no** form of this command.

```
authentication mac-move permit
no authentication mac-move permit
```

Syntax Description This command has no arguments or keywords.

Command Default MAC move is disabled.

Command Modes Global configuration

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines The command enables authenticated hosts to move between ports on a device. For example, if there is a device between an authenticated host and port, and that host moves to another port, the authentication session is deleted from the first port, and the host is reauthenticated on the new port.

If MAC move is disabled, and an authenticated host moves to another port, it is not reauthenticated, and a violation error occurs.

This example shows how to enable MAC move on a device:

```
Device(config)# authentication mac-move permit
```

authentication priority

To add an authentication method to the port-priority list, use the **authentication priority** command in interface configuration mode. To return to the default, use the **no** form of this command.

```
authentication priority [dot1x | mab] {webauth}
no authentication priority [dot1x | mab] {webauth}
```

Syntax Description	dot1x	(Optional) Adds 802.1x to the order of authentication methods.
	mab	(Optional) Adds MAC authentication bypass (MAB) to the order of authentication methods.
	webauth	Adds web authentication to the order of authentication methods.

Command Default The default priority is 802.1x authentication, followed by MAC authentication bypass and web authentication.

Command Modes Interface configuration

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines Ordering sets the order of methods that the switch attempts when trying to authenticate a new device is connected to a port.

When configuring multiple fallback methods on a port, set web authentication (webauth) last.

Assigning priorities to different authentication methods allows a higher-priority method to interrupt an in-progress authentication method with a lower priority.



Note If a client is already authenticated, it might be reauthenticated if an interruption from a higher-priority method occurs.

The default priority of an authentication method is equivalent to its position in execution-list order: 802.1x authentication, MAC authentication bypass (MAB), and web authentication. Use the **dot1x**, **mab**, and **webauth** keywords to change this default order.

This example shows how to set 802.1x as the first authentication method and web authentication as the second authentication method:

```
Device(config-if)# authentication priority dot1x webauth
```

This example shows how to set MAB as the first authentication method and web authentication as the second authentication method:

```
Device(config-if)# authentication priority mab webauth
```

Related Commands	Command	Description
	authentication control-direction	Configures the port mode as unidirectional or bidirectional.
	authentication event fail	Specifies how the Auth Manager handles authentication failures as a result of unrecognized user credentials.
	authentication event no-response action	Specifies how the Auth Manager handles authentication failures as a result of a nonresponsive host.

authentication priority

Command	Description
authentication event server alive action reinitialize	Reinitializes an authorized Auth Manager session when a previously unreachable authentication, authorization, and accounting server becomes available.
authentication event server dead action authorize	Authorizes Auth Manager sessions when the authentication, authorization, and accounting server becomes unreachable.
authentication fallback	Enables a web authentication fallback method.
authentication host-mode	Allows hosts to gain access to a controlled port.
authentication open	Enables open access on a port.
authentication order	Specifies the order in which the Auth Manager attempts to authenticate a client on a port.
authentication periodic	Enables automatic reauthentication on a port.
authentication port-control	Configures the authorization state of a controlled port.
authentication timer inactivity	Configures the time after which an inactive Auth Manager session is terminated.
authentication timer reauthenticate	Specifies the period of time between which the Auth Manager attempts to reauthenticate authorized ports.
authentication timer restart	Specifies the period of time after which the Auth Manager attempts to authenticate an unauthorized port.
authentication violation	Specifies the action to be taken when a security violation occurs on a port.
mab	Enables MAC authentication bypass on a port.
show authentication registrations	Displays information about the authentication methods that are registered with the Auth Manager.
show authentication sessions	Displays information about current Auth Manager sessions.
show authentication sessions interface	Displays information about the Auth Manager for a given interface.

authentication violation

To configure the violation modes that occur when a new device connects to a port or when a new device connects to a port after the maximum number of devices are connected to that port, use the **authentication violation** command in interface configuration mode.

```
authentication violation { protect | replace | restrict | shutdown }
no authentication violation { protect | replace | restrict | shutdown }
```

Syntax Description	protect	Drops unexpected incoming MAC addresses. No syslog errors are generated.
	replace	Removes the current session and initiates authentication with the new host.
	restrict	Generates a syslog error when a violation error occurs.
	shutdown	Error-disables the port or the virtual port on which an unexpected MAC address occurs.
Command Default	Authentication violation shutdown mode is enabled.	
Command Modes	Interface configuration	
Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines Use the **authentication violation** command to specify the action to be taken when a security violation occurs on a port.

This example shows how to configure an IEEE 802.1x-enabled port as error-disabled and to shut down when a new device connects it:

```
Device(config-if)# authentication violation shutdown
```

This example shows how to configure an 802.1x-enabled port to generate a system error message and to change the port to restricted mode when a new device connects to it:

```
Device(config-if)# authentication violation restrict
```

This example shows how to configure an 802.1x-enabled port to ignore a new device when it connects to the port:

```
Device(config-if)# authentication violation protect
```

cisp enable

This example shows how to configure an 802.1x-enabled port to remove the current session and initiate authentication with a new device when it connects to the port:

```
Device(config-if)# authentication violation replace
```

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

cisp enable

To enable Client Information Signaling Protocol (CISP) on a switch so that it acts as an authenticator to a supplicant switch and a supplicant to an authenticator switch, use the **cisp enable** global configuration command.

```
cisp enable
no cisp enable
```

Syntax Description This command has no arguments or keywords.

Command Default No default behavior or values.

Command Modes Global configuration

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.
		This command was reintroduced. This command was not supported in and

Usage Guidelines The link between the authenticator and supplicant switch is a trunk. When you enable VTP on both switches, the VTP domain name must be the same, and the VTP mode must be server.

To avoid the MD5 checksum mismatch error when you configure VTP mode, verify that:

- VLANs are not configured on two different switches, which can be caused by two VTP servers in the same domain.
- Both switches have different configuration revision numbers.

This example shows how to enable CISP:

```
Device(config)# cisp enable
```

Related Commands	Command	Description
	dot1x credentialsprofile	Configures a profile on a supplicant switch.

Command	Description
dot1x supplicant force-multicast	Forces 802.1X supplicant to send multicast packets.
dot1x supplicant controlled transient	Configures controlled access by 802.1X supplicant.
show cisp	Displays CISP information for a specified interface.

clear errdisable interface vlan

To reenable a VLAN that was error-disabled, use the **clear errdisable interface** command in privileged EXEC mode.

clear errdisable interface *interface-id* vlan [vlist]

Syntax Description	<i>interface-id</i>	Specifies an interface.
	<i>vlan list</i>	(Optional) Specifies a list of VLANs to be reenabled. If a VLAN list is not specified, then all VLANs are reenabled.

Command Default No default behavior or values.

Command Modes Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines You can reenable a port by using the **shutdown** and **no shutdown** interface configuration commands, or you can clear error-disable for VLANs by using the **clear errdisable** interface command.

This example shows how to reenable all VLANs that were error-disabled on Gigabit Ethernet port 4/0/2:

```
Device# clear errdisable interface gigabitethernet4/0/2 vlan
```

Related Commands	Command	Description
	errdisable detect cause	Enables error-disabled detection for a specific cause or all causes.
	errdisable recovery	Configures the recovery mechanism variables.
	show errdisable detect	Displays error-disabled detection status.
	show errdisable recovery	Displays error-disabled recovery timer information.

clear mac address-table

Command	Description
show interfaces status err-disabled	Displays interface status of a list of interfaces in error-disabled state.

clear mac address-table

To delete from the MAC address table a specific dynamic address, all dynamic addresses on a particular interface, all dynamic addresses on stack members, or all dynamic addresses on a particular VLAN, use the **clear mac address-table** command in privileged EXEC mode. This command also clears the MAC address notification global counters.

```
clear mac address-table {dynamic [address mac-addr | interface interface-id | vlan vlan-id]
| move update | notification}
```

Syntax Description	
dynamic	Deletes all dynamic MAC addresses.
address mac-addr	(Optional) Deletes the specified dynamic MAC address.
interface interface-id	(Optional) Deletes all dynamic MAC addresses on the specified physical port or port channel.
vlan vlan-id	(Optional) Deletes all dynamic MAC addresses for the specified VLAN. The range is 1 to 4094.
move update	Clears the MAC address table move-update counters.
notification	Clears the notifications in the history table and reset the counters.

Command Default	No default behavior or values.				
Command Modes	Privileged EXEC				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				

Usage Guidelines	You can verify that the information was deleted by entering the show mac address-table privileged EXEC command.
-------------------------	--

This example shows how to remove a specific MAC address from the dynamic address table:

```
Device# clear mac address-table dynamic address 0008.0070.0007
```

Related Commands	Command	Description
	mac address-table notification	Enables the MAC address notification feature.
	mac address-table move update {receive transmit}	Configures MAC address-table move update on the switch.
	show mac address-table	Displays the MAC address table static and dynamic entries.
	show mac address-table move update	Displays the MAC address-table move update information on the switch.
	show mac address-table notification	Displays the MAC address notification settings for all interfaces or on the specified interface when the interface keyword is appended.
	snmp trap mac-notification change	Enables the SNMP MAC address notification trap on a specific interface.

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 Everest 16.6.1	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.

Command	Description
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.

cts manual

To manually enable an interface for Cisco TrustSec Security (CTS), use the **cts manual** command in interface configuration mode.

cts manual

Syntax Description This command has no arguments or keywords.

Command Default Disabled

Command Modes Interface configuration (config-if)

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was modified with additional options.
	Cisco IOS XE 3.7E	This command was introduced.

Usage Guidelines Use the **cts manual** command to enter the TrustSec manual interface configuration in which policies and the Security Association Protocol (SAP) are configured on the link.

When **cts manual** command is configured, 802.1X authentication is not performed on the link. Use the **policy** subcommand to define and apply policies on the link. By default no policy is applied. To configure MACsec link-to-link encryption, the SAP negotiation parameters must be defined. By default SAP is not enabled. The same SAP Pairwise master key (PMK) should be configured on both sides of the link (that is, a shared secret).

Examples

The following example shows how to enter the Cisco TrustSec manual mode:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet 0
```

```
Switch(config-if)# cts manual
Switch(config-if-cts-manual)#
```

The following example shows how to remove the CTS manual configuration from an interface:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet 0
Switch(config-if)# no cts manual
```

Related Commands	Command	Description
	propagate sgt (cts manual)	Enables Security Group Tag (SGT) propagation at Layer 2 on Cisco TrustSec Security (CTS) interfaces.
	sap mode-list (cts manual)	Manually specifies the PMK and the SAP authentication and encryption modes to negotiate MACsec link encryption between two interfaces.
	show cts interface	Displays Cisco TrustSec interface configuration statistics.

cts role-based enforcement

To enable Cisco TrustSec role-based (security group) access control enforcement, use the **cts role-based enforcement** command in global configuration mode. To disable the configuration, use the **no** form of this command.

```
cts role-based enforcement [{logging-interval interval | vlan-list {all | vlan-ID [,{,}] [-]}]}
no cts role-based enforcement [{logging-interval interval | vlan-list {all | vlan-ID [,{,}] [-]}]}
```

Syntax Description	logging-interval interval (Optional) Configures a logging interval for a security group access control list (SGACL). Valid values for the <i>interval</i> argument are from 5 to 86400 seconds. The default is 300 seconds
	vlan-list (Optional) Configures VLANs on which role-based ACLs are enforced.
	all (Optional) Specifies all VLANs.
	vlan-ID (Optional) VLAN ID. Valid values are from 1 to 4094.
	, (Optional) Specifies another VLAN separated by a comma.
	- (Optional) Specifies a range of VLANs separated by a hyphen.

Command Default Role-based access control is not enforced.

Command Modes Global configuration (config)

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

Usage Guidelines

Note RBACL and SGACL are used interchangeably.

Use the **cts role-based enforcement** command to globally enable or disable SGACL enforcement for Cisco TrustSec-enabled interfaces in the system.

The default interval after which log for a given flow is printed is 300 seconds. Use the **logging-interval** keyword to change the default interval. Logging is only triggered when the Cisco ACE Application Control Engine has the **logging** keyword.

SGACL enforcement is not enabled by default on VLANs. Use the **cts role-based enforcement vlan-list** command to enable or disable SGACL enforcement for Layer 2 switched packets and for Layer 3 switched packets on an switched virtual interface (SVI).

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

When a VLAN in which a SGACL is enforced has an active SVI, the SGACL is enforced for both Layer 2 and Layer 3 switched packets within that VLAN. Without an SVI, the SGACL is enforced only for Layer 2 switched packets, because no Layer 3 switching is possible within a VLAN without an SVI.

The following example shows configure an SGACL logging interval:

```
Switch(config)# cts role-based enforcement logging-interval 90
Switch(config)# logging rate-limit

May 27 10:19:21.509: %RBM-6-SGACLHIT:
ingress_interface='GigabitEthernet1/0/2' sgacl_name='sgacl2' action='Deny'
protocol='icmp' src-ip='16.16.1.3' src-port='8' dest-ip='17.17.1.2' dest-port='0'
sgt='101' dgt='202' logging_interval_hits='5'
```

Related Commands

Command	Description
logging rate-limit	Limits the rate of messages logged per second.
show cts role-based permissions	Displays the SGACL permission list.

cts role-based l2-vrf

To select a virtual routing and forwarding (VRF) instance for Layer 2 VLANs, use the **cts role-based l2-vrf** command in global configuration mode. To remove the configuration, use the **no** form of this command.

```
cts role-based l2-vrf vrf-name vlan-list {all vlan-ID} [{,}] [{-}]
no cts role-based l2-vrf vrf-name vlan-list {all vlan-ID} [{,}] [{-}]
```

Syntax Description

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.

<i>vlan-ID</i>	VLAN ID. Valid values are from 1 to 4094.
,	(Optional) Specifies another VLAN separated by a comma.
-	(Optional) Specifies a range of VLANs separated by a hyphen.

Command Default VRF instances are not selected.

Command Modes Global configuration (config)

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

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

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

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

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

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

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

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

```
Switch(config)# cts role-based l2-vrf vrf1 vlan-list 20
```

The following example shows how to configure an SVI interface and associate a VRF instance:

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

Related Commands	Command	Description
	interface vlan	Configures a VLAN interface.

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

cts role-based monitor

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

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

Syntax Description	all Monitors permissions for all source tags to all destination tags. permissions Monitors permissions from a source tags to a destination tags. default Monitors the default permission list. from Specifies the source group tag for filtered traffic. sgt Security Group Tag (SGT). Valid values are from 2 to 65519. unknown Specifies an unknown source or destination group tag (DST). ipv4 (Optional) Specifies the IPv4 protocol.				
Command Default	Role-based access control monitoring is not enabled.				
Command Modes	Global configuration (config)				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Denali 16.3.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Denali 16.3.1	This command was introduced.
Release	Modification				
Cisco IOS XE Denali 16.3.1	This command was introduced.				

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

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

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

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

cts role-based permissions

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

```
cts role-based permissions {default ipv4 | from {sgt | unknown} to {sgt | unknown} {ipv4}
{rbac-name [{rbac-name....}]}}

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

Syntax Description	default Specifies the default permissions list. Every cell (an SGT pair) for which, security group access control list (SGACL) permission is not configured statically or dynamically falls under the default category.				
ipv4	Specifies the IPv4 protocol.				
from	Specifies the source group tag of the filtered traffic.				
<i>sgt</i>	Security Group Tag (SGT). Valid values are from 2 to 65519.				
unknown	Specifies an unknown source or destination group tag.				
<i>rbac-name</i>	Role-based access control list (RBACL) or SGACL name. Up to 16 SGACLs can be specified in the configuration.				
Command Default	Permissions from a source group to a destination group is not enabled.				
Command Modes	Global configuration (config)				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Denali 16.3.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Denali 16.3.1	This command was introduced.
Release	Modification				
Cisco IOS XE Denali 16.3.1	This command was introduced.				

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

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

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

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

delay-protection

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

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 Everest 16.6.1	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** MAC access-list configuration command on the switch stack or on a standalone switch. To remove a deny condition from the named MAC access list, use the **no** form of this command.

```
deny {any | host src-MAC-addr | src-MAC-addr mask} {any | host dst-MAC-addr | dst-MAC-addr mask} [type mask | aarp | amber | appletalk | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000 | etype-8042 | lat | lave-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 | lave-sca | lsap lsap mask | mop-console | mop-dump | msdos | mumps | netbios | vines-echo | vines-ip | xns-idp] [cos cos]
```

Syntax Description		
	any	Denies any source or destination MAC address.
	host src-MAC-addr src-MAC-addr mask	Defines a host MAC address and optional subnet mask. If the source address for a packet matches the defined address, non-IP traffic from that address is denied.
	host dst-MAC-addr dst-MAC-addr mask	Defines a destination MAC address and optional subnet mask. If the destination address for a packet matches the defined address, non-IP traffic to that address is denied.
	type mask	(Optional) Specifies the EtherType number of a packet with Ethernet II or SNAP encapsulation to identify the protocol of the packet. The type is 0 to 65535, specified in hexadecimal. The mask is a mask of don't care bits applied to the EtherType before testing for a match.
	aarp	(Optional) Specifies EtherType AppleTalk Address Resolution Protocol that maps a data-link address to a network address.
	amber	(Optional) Specifies EtherType DEC-Amber.
	appletalk	(Optional) Specifies EtherType AppleTalk/EtherTalk.
	dec-spanning	(Optional) Specifies EtherType Digital Equipment Corporation (DEC) spanning tree.
	decnet-iv	(Optional) Specifies EtherType DECnet Phase IV protocol.
	diagnostic	(Optional) Specifies EtherType DEC-Diagnostic.

deny (MAC access-list configuration)

dsm	(Optional) Specifies EtherType DEC-DSM.
etype-6000	(Optional) Specifies EtherType 0x6000.
etype-8042	(Optional) Specifies EtherType 0x8042.
lat	(Optional) Specifies EtherType DEC-LAT.
lavc-sca	(Optional) Specifies EtherType DEC-LAVC-SCA.
lsap <i>lsap-number mask</i>	(Optional) Specifies the LSAP number (0 to 65535) of a packet with 802.2 encapsulation to identify the protocol of the packet. <i>mask</i> is a mask of don't care bits applied to the LSAP number before testing for a match.
mop-console	(Optional) Specifies EtherType DEC-MOP Remote Console.
mop-dump	(Optional) Specifies EtherType DEC-MOP Dump.
msdos	(Optional) Specifies EtherType DEC-MSDOS.
mumps	(Optional) Specifies EtherType DEC-MUMPS.
netbios	(Optional) Specifies EtherType DEC- Network Basic Input/Output System (NetBIOS).
vines-echo	(Optional) Specifies EtherType Virtual Integrated Network Service (VINES) Echo from Banyan Systems.
vines-ip	(Optional) Specifies EtherType VINES IP.
xns-idp	(Optional) Specifies EtherType Xerox Network Systems (XNS) protocol suite (0 to 65535), an arbitrary EtherType in decimal, hexadecimal, or octal.
cos <i>cos</i>	(Optional) Specifies a class of service (CoS) number from 0 to 7 to set priority. Filtering on CoS can be performed only in hardware. A warning message reminds the user if the cos option is configured.

Command Default

This command has no defaults. However, the default action for a MAC-named ACL is to deny.

Command Modes

Mac-access list configuration

Command History**Release****Modification**

Cisco IOS XE Everest 16.6.1

This command was introduced.

Usage Guidelines

You enter MAC-access list configuration mode by using the **mac access-list extended** global configuration command.

If you use the **host** keyword, you cannot enter an address mask; if you do not use the **host** keyword, you must enter an address mask.

When an access control entry (ACE) is added to an access control list, an implied **deny-any-any** condition exists at the end of the list. That is, if there are no matches, the packets are denied. However, before the first ACE is added, the list permits all packets.

To filter IPX traffic, you use the *type mask* or **Isap lsap mask** keywords, depending on the type of IPX encapsulation being used. Filter criteria for IPX encapsulation types as specified in Novell terminology and Cisco IOS terminology are listed in the table.

Table 163: IPX Filtering Criteria

IPX Encapsulation Type		Filter Criterion
Cisco IOS Name	Novel Name	
arpa	Ethernet II	EtherType 0x8137
snap	Ethernet-snap	EtherType 0x8137
sap	Ethernet 802.2	LSAP 0xE0E0
novell-ether	Ethernet 802.3	LSAP 0xFFFF

This example shows how to define the named MAC extended access list to deny NETBIOS traffic from any source to MAC address 00c0.00a0.03fa. Traffic matching this list is denied.

```
Device(config-ext-macl)# deny any host 00c0.00a0.03fa netbios.
```

This example shows how to remove the deny condition from the named MAC extended access list:

```
Device(config-ext-macl)# no deny any 00c0.00a0.03fa 0000.0000.0000 netbios.
```

This example denies all packets with EtherType 0x4321:

```
Device(config-ext-macl)# deny any any 0x4321 0
```

You can verify your settings by entering the **show access-lists** privileged EXEC command.

Related Commands

Command	Description
mac access-list extended	Creates an access list based on MAC addresses for non-IP traffic.
permit	Permits from the MAC access-list configuration. Permits non-IP traffic to be forwarded if conditions are matched.

device-role (IPv6 snooping)

Command	Description
show access-lists	Displays access control lists configured on a switch.

device-role (IPv6 snooping)

To specify the role of the device attached to the port, use the **device-role** command in IPv6 snooping configuration mode.

device-role {node | switch}

Syntax Description

node Sets the role of the attached device to node.

switch Sets the role of the attached device to switch.

Command Default

The device role is node.

Command Modes

IPv6 snooping configuration

Command History
Release
Modification

Cisco IOS XE Everest 16.6.1

This command was introduced.

Usage Guidelines

The **device-role** command specifies the role of the device attached to the port. By default, the device role is node.

The **switch** keyword indicates that the remote device is a switch and that the local switch is now operating in multiswitch mode; binding entries learned from the port will be marked with trunk_port preference level. If the port is configured as a trust-port, binding entries will be marked with trunk_trusted_port preference level.

This example shows how to define an IPv6 snooping policy name as policy1, place the device in IPv6 snooping configuration mode, and configure the device as the node:

```
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# device-role node
```

device-role (IPv6 nd inspection)

To specify the role of the device attached to the port, use the **device-role** command in neighbor discovery (ND) inspection policy configuration mode.

device-role {host | switch}

Syntax Description

host Sets the role of the attached device to host.

switch Sets the role of the attached device to switch.

Command Default	The device role is host.				
Command Modes	ND inspection policy configuration				
Command History	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; padding-bottom: 5px;">Release</th><th style="text-align: right; padding-bottom: 5px;">Modification</th></tr> </thead> <tbody> <tr> <td style="padding-top: 5px;">Cisco IOS XE Everest 16.6.1</td><td style="text-align: right; padding-top: 5px;">This command was introduced.</td></tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				
Usage Guidelines	<p>The device-role command specifies the role of the device attached to the port. By default, the device role is host, and therefore all the inbound router advertisement and redirect messages are blocked.</p> <p>The switch keyword indicates that the remote device is a switch and that the local switch is now operating in multiswitch mode; binding entries learned from the port will be marked with <code>trunk_port</code> preference level. If the port is configured as a trust-port, binding entries will be marked with <code>trunk_trusted_port</code> preference level.</p> <p>The following example defines a Neighbor Discovery Protocol (NDP) policy name as <code>policy1</code>, places the device in ND inspection policy configuration mode, and configures the device as the host:</p> <pre>Device(config)# ipv6 nd inspection policy policy1 Device(config-nd-inspection)# device-role host</pre>				

device-tracking policy

To configure a Switch Integrated Security Features (SISF)-based IP device tracking policy, use the **device-tracking** command in global configuration mode. To delete a device tracking policy, use the **no** form of this command.

device -tracking policy *policy-name*
no device-tracking policy *policy-name*

Syntax Description	<i>policy-name</i> User-defined name of the device tracking policy. The policy name can be a symbolic string (such as <code>Engineering</code>) or an integer (such as <code>0</code>).				
Command Default	A device tracking policy is not configured.				
Command Modes	Global configuration				
Command History	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; padding-bottom: 5px;">Release</th><th style="text-align: right; padding-bottom: 5px;">Modification</th></tr> </thead> <tbody> <tr> <td style="padding-top: 5px;"></td><td style="text-align: right; padding-top: 5px;">This command was introduced.</td></tr> </tbody> </table>	Release	Modification		This command was introduced.
Release	Modification				
	This command was introduced.				

Usage Guidelines	<p>Use the SISF-based device-tracking policy command to create a device tracking policy. When the device-tracking policy command is enabled, the configuration mode changes to device-tracking configuration mode. In this mode, the administrator can configure the following first-hop security commands:</p> <ul style="list-style-type: none"> • (Optional) device-role{node} switch}—Specifies the role of the device attached to the port. Default is <code>node</code>.
-------------------------	--

dot1x critical (global configuration)

- (Optional) **limit address-count value**—Limits the number of addresses allowed per target.
- (Optional) **no**—Negates a command or sets it to defaults.
- (Optional) **destination-glean{recovery| log-only}[dhcp]**—Enables binding table recovery by data traffic source address gleaning.
- (Optional) **data-glean{recovery| log-only}[dhcp | ndp]**—Enables binding table recovery using source or data address gleaning.
- (Optional) **security-level{glean|guard|inspect}**—Specifies the level of security enforced by the feature. Default is **guard**.
 - glean**—Gleans addresses from messages and populates the binding table without any verification.
 - guard**—Gleans addresses and inspects messages. In addition, it rejects RA and DHCP server messages. This is the default option.
 - inspect**—Gleans addresses, validates messages for consistency and conformance, and enforces address ownership.
- (Optional) **tracking {disable | enable}**—Specifies a tracking option.
- (Optional) **trusted-port**—Sets up a trusted port. It disables the guard on applicable targets. Bindings learned through a trusted port have preference over bindings learned through any other port. A trusted port is given preference in case of a collision while making an entry in the table.

This example shows how to configure an a device-tracking policy:

```
Device(config)# device-tracking policy policy1
Device(config-device-tracking)# trusted-port
```

dot1x critical (global configuration)

To configure the IEEE 802.1X critical authentication parameters, use the **dot1x critical** command in global configuration mode.

dot1x critical eapol

Syntax Description	eapol Specifies that the switch send an EAPOL-Success message when the switch successfully authenticates the critical port.				
Command Default	eapol is disabled				
Command Modes	Global configuration				
Command History	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; width: 50%;">Release</th><th style="text-align: left;">Modification</th></tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td><td>This command was introduced.</td></tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				

This example shows how to specify that the switch sends an EAPOL-Success message when the switch successfully authenticates the critical port:

```
Device(config)# dot1x critical eapol
```

dot1x 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						
Command History	<table border="1"> <thead> <tr> <th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td><td>This command was introduced.</td></tr> <tr> <td></td><td>This command was reintroduced. This command was not supported in and</td></tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.		This command was reintroduced. This command was not supported in and
Release	Modification						
Cisco IOS XE Everest 16.6.1	This command was introduced.						
	This command was reintroduced. This command was not supported in and						

Usage Guidelines Use the **no dot1x pae** interface configuration command to disable IEEE 802.1x authentication on the port.

When you configure IEEE 802.1x authentication on a port, such as by entering the **dot1x port-control** interface configuration command, the switch automatically configures the port as an IEEE 802.1x authenticator. After the **no dot1x pae** interface configuration command is entered, the Authenticator PAE operation is disabled.

The following example shows that the interface has been set to act as a supplicant:

```
Device(config)# interface g1/0/3
Device(config-if)# dot1x pae supplicant
```

dot1x supplicant controlled transient

dot1x supplicant controlled transient

To control access to an 802.1x supplicant port during authentication, use the **dot1x supplicant controlled transient** command in global configuration mode. To open the supplicant port during authentication, use the **no** form of this command

dot1x supplicant controlled transient
no dot1x supplicant controlled transient

Syntax Description	This command has no arguments or keywords.	
Command Default	Access is allowed to 802.1x supplicant ports during authentication.	
Command Modes	Global configuration	
Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.
		This command was reintroduced. This command was not supported in and

Usage Guidelines In the default state, when you connect a supplicant switch to an authenticator switch that has BPCU guard enabled, the authenticator port could be error-disabled if it receives a Spanning Tree Protocol (STP) bridge protocol data unit (BPDU) packets before the supplicant switch has authenticated. Beginning with Cisco IOS Release 15.0(1)SE, you can control traffic exiting the supplicant port during the authentication period. Entering the **dot1x supplicant controlled transient** global configuration command temporarily blocks the supplicant port during authentication to ensure that the authenticator port does not shut down before authentication completes. If authentication fails, the supplicant port opens. Entering the **no dot1x supplicant controlled transient** global configuration command opens the supplicant port during the authentication period. This is the default behavior.

We strongly recommend using the **dot1x supplicant controlled transient** command on a supplicant switch when BPDU guard is enabled on the authenticator switch port with the **spanning-tree bpduguard enable** interface configuration command.

This example shows how to control access to 802.1x supplicant ports on a switch during authentication:

```
Device(config)# dot1x supplicant controlled transient
```

dot1x supplicant force-multicast

To force a supplicant switch to send only multicast Extensible Authentication Protocol over LAN (EAPOL) packets whenever it receives multicast or unicast EAPOL packets, use the **dot1x supplicant force-multicast** command in global configuration mode. To return to the default setting, use the **no** form of this command.

```
dot1x supplicant force-multicast
no dot1x supplicant force-multicast
```

Syntax Description

This command has no arguments or keywords.

Command Default

The supplicant switch sends unicast EAPOL packets when it receives unicast EAPOL packets. Similarly, it sends multicast EAPOL packets when it receives multicast EAPOL packets.

Command Modes

Global configuration

Command History

	Release	Modification
Cisco IOS XE Everest 16.6.1		This command was introduced.
		This command was reintroduced. This command was not supported in and

Usage Guidelines

Enable this command on the supplicant switch for Network Edge Access Topology (NEAT) to work in all host modes.

This example shows how force a supplicant switch to send multicast EAPOL packets to the authenticator switch:

```
Device(config)# dot1x supplicant force-multicast
```

Related Commands

Command	Description
cisp enable	Enable Client Information Signalling Protocol (CISP) on a switch so that it acts as an authenticator to a supplicant switch.
dot1x credentials	Configure the 802.1x supplicant credentials on the port.
dot1x pae supplicant	Configure an interface to act only as a supplicant.

dot1x test eapol-capable

To monitor IEEE 802.1x activity on all the switch ports and to display information about the devices that are connected to the ports that support IEEE 802.1x, use the **dot1x test eapol-capable** command in privileged EXEC mode on the switch stack or on a standalone switch.

```
dot1x test eapol-capable [interface interface-id]
```

Syntax Description

interface interface-id	(Optional) Port to be queried.
-------------------------------	--------------------------------

dot1x test timeout

Command Default	There is no default setting.					
Command Modes	Privileged EXEC					
Command History	Release	Modification				
	Cisco IOS XE Everest 16.6.1	This command was introduced.				
Usage Guidelines	<p>Use this command to test the IEEE 802.1x capability of the devices connected to all ports or to specific ports on a switch.</p> <p>There is not a no form of this command.</p> <p>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:</p> <pre>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</pre>					
Related Commands	<table border="1"> <thead> <tr> <th>Command</th><th>Description</th></tr> </thead> <tbody> <tr> <td>dot1x test timeout <i>timeout</i></td><td>Configures the timeout used to wait for EAPOL response to an IEEE 802.1x readiness query.</td></tr> </tbody> </table>		Command	Description	dot1x test timeout <i>timeout</i>	Configures the timeout used to wait for EAPOL response to an IEEE 802.1x readiness query.
Command	Description					
dot1x test timeout <i>timeout</i>	Configures the timeout used to wait for EAPOL response to an IEEE 802.1x readiness query.					

dot1x test timeout

To configure the timeout used to wait for EAPOL response from a port being queried for IEEE 802.1x readiness, use the **dot1x test timeout** command in global configuration mode on the switch stack or on a standalone switch.

dot1x test timeout *timeout*

Syntax Description	<i>timeout</i>	Time in seconds to wait for an EAPOL response. The range is from 1 to 65535 seconds.
Command Default	The default setting is 10 seconds.	
Command Modes	Global configuration	
Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.
Usage Guidelines	Use this command to configure the timeout used to wait for EAPOL response.	

There is not a no form of this command.

This example shows how to configure the switch to wait 27 seconds for an EAPOL response:

```
Device# dot1x test timeout 27
```

You can verify the timeout configuration status by entering the **show run** privileged EXEC command.

Related Commands	Command	Description
	dot1x test eapol-capable [interface <i>interface-id</i>]	Checks for IEEE 802.1x readiness on devices connected to all or to specified IEEE 802.1x-capable ports.

dot1x timeout

To configure the value for retry timeouts, use the **dot1x timeout** command in global configuration or interface configuration mode. To return to the default value for retry timeouts, use the **no** form of this command.

```
dot1x timeout { auth-period seconds | held-period seconds | quiet-period seconds | ratelimit-period seconds | server-timeout seconds | start-period seconds | supp-timeout seconds | tx-period seconds }
```

Syntax Description	auth-period <i>seconds</i> held-period <i>seconds</i> quiet-period <i>seconds</i> ratelimit-period <i>seconds</i>	Configures the time, in seconds for which a supplicant will stay in the HELD state (that is, the length of time it will wait before trying to send the credentials again after a failed attempt). The range is from 1 to 65535. The default is 30. 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 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 Throttles the EAP-START packets that are sent from misbehaving client PCs (for example, PCs that send EAP-START packets that result in the wasting of switch processing power). <ul style="list-style-type: none"> • The authenticator ignores EAPOL-Start packets from clients that have successfully authenticated for the rate-limit period duration. • The range is from 1 to 65535. By default, rate limiting is disabled.
---------------------------	--	--

dot1x timeout

server-timeout <i>seconds</i>	Configures the interval, in seconds, between two successive EAPOL-Start frames when they are being retransmitted. <ul style="list-style-type: none">• The range is from 1 to 65535. The default is 30. If the server does not send a response to an 802.1X packet within the specified period, the packet is sent again.
start-period <i>seconds</i>	Configures the interval, in seconds, between two successive EAPOL-Start frames when they are being retransmitted. The range is from 1 to 65535. The default is 30. In Cisco IOS Release 15.2(5)E, this command is only available in the supplicant mode. If the command is applied in any other mode, the command misses from the configuration.
supp-timeout <i>seconds</i>	Sets the authenticator-to-suppliant retransmission time for all EAP messages other than EAP Request ID. The range is from 1 to 65535. The default is 30.
tx-period <i>seconds</i>	Configures the number of seconds between retransmission of EAP request ID packets (assuming that no response is received) to the client. <ul style="list-style-type: none">• The range is from 1 to 65535. The default is 30.• If an 802.1X packet is sent to the supplicant and the supplicant does not send a response after the retry period, the packet will be sent again.

Command Default Periodic reauthentication and periodic rate-limiting are done.

Command Modes Interface configuration

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines You should change the default value of this command only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain clients and authentication servers.

The **dot1x timeout reauth-period** interface configuration command affects the behavior of the switch only if you have enabled periodic re-authentication by using the **dot1x reauthentication** interface configuration command.

During the quiet period, the switch does not accept or initiate any authentication requests. If you want to provide a faster response time to the user, enter a number smaller than the default.

When the **ratelimit-period** is set to 0 (the default), the switch does not ignore EAPOL packets from clients that have been successfully authenticated and forwards them to the RADIUS server.

The following example shows that various 802.1X retransmission and timeout periods have been set:

```

Device(config)# configure terminal
Device(config)# interface g1/0/3
Device(config-if)# dot1x port-control auto
Device(config-if)# dot1x timeout auth-period 2000
Device(config-if)# dot1x timeout held-period 2400
Device(config-if)# dot1x timeout quiet-period 600
Device(config-if)# dot1x timeout start-period 90
Device(config-if)# dot1x timeout supp-timeout 300
Device(config-if)# dot1x timeout tx-period 60
Device(config-if)# dot1x timeout server-timeout 60

```

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 <i>connection-timeout-value</i> idletimeout <i>idle-timeout-value</i> ip { radius source-interface <i>interface-name</i> vrf forwarding <i>forwarding-table-name</i> } port <i>port-number</i> retries <i>number-of-connection-retries</i> trustpoint { client <i>trustpoint name</i> server <i>trustpoint name</i> }	(Optional) Configures the DTLS connection timeout value. (Optional) Configures the DTLS idle timeout value. (Optional) Configures IP source parameters. (Optional) Configures the DTLS port number. (Optional) Configures the number of DTLS connection retries. (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)

epm access-control open

Command History

Release	Modification
Cisco IOS XE Everest 16.6.1	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.

epm access-control open

To configure an open directive for ports that do not have an access control list (ACL) configured, use the **epm access-control open** command in global configuration mode. To disable the open directive, use the **no** form of this command.

epm access-control open
no epm access-control open

Syntax Description

This command has no arguments or keywords.

Command Default

The default directive applies.

Command Modes

Global configuration

Command History

Release	Modification
---------	--------------

Cisco IOS XE Everest 16.6.1 This command was introduced.

Usage Guidelines

Use this command to configure an open directive that allows hosts without an authorization policy to access ports configured with a static ACL. If you do not configure this command, the port applies the policies of the configured ACL to the traffic. If no static ACL is configured on a port, both the default and open directives allow access to the port.

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

This example shows how to configure an open directive.

```
Device(config)# epm access-control open
```

Related Commands	Command	Description
	show running-config	Displays the contents of the current running configuration file.

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 Everest 16.6.1	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.

ip access-list role-based

Command	Description
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 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)

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

Usage Guidelines For SGACL logging, you must configure the **permit ip log** command. Also, this command must be configured in Cisco Identity Services Engine (ISE) to enable logging for dynamic SGACLs.

The following example shows how to define an SGACL that can be applied to IPv4 traffic and enter role-based access list configuration mode:

```
Switch(config)# ip access-list role-based rbacl1
Switch(config-rb-acl)# permit ip log
```

Related Commands	Command	Description
	permit ip log	Permits logging that matches the configured entry.
	show ip access-list	Displays contents of all current IP access lists.

ip admission

To enable web authentication, use the **ip admission** command in interface configuration mode. You can also use this command in fallback-profile configuration mode. To disable web authentication, use the **no** form of this command.

ip admission rule
no ip admission rule

Syntax Description	<i>rule</i> IP admission rule name.				
Command Default	Web authentication is disabled.				
Command Modes	Interface configuration Fallback-profile configuration				
Command History	<table border="1"> <thead> <tr> <th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td><td>This command was introduced.</td></tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				

Usage Guidelines The **ip admission** command applies a web authentication rule to a switch port.

This example shows how to apply a web authentication rule to a switchport:

```
Device# configure terminal
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip admission rule1
```

This example shows how to apply a web authentication rule to a fallback profile for use on an IEEE 802.1x enabled switch port.

```
Device# configure terminal
Device(config)# fallback profile profile1
Device(config-fallback-profile)# ip admission rule1
```

ip admission name

To enable web authentication, use the **ip admission name** command in global configuration mode. To disable web authentication, use the **no** form of this command.

ip admission name name {consent | proxy http} [absolute timer minutes | inactivity-time minutes | list {acl | acl-name} | service-policy type tag service-policy-name]
no ip admission name name {consent | proxy http} [absolute timer minutes | inactivity-time minutes | list {acl | acl-name} | service-policy type tag service-policy-name]

ip admission 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 <i>admission-name</i> 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 <i>policynam</i> command, keyword, and argument. This policy map is used to apply the actions on the host when a tag is received.

Command Default	Web authentication is disabled.
------------------------	---------------------------------

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

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines	The ip admission name command globally enables web authentication on a switch.
-------------------------	---

After you enable web authentication on a switch, use the **ip access-group in** and **ip admission web-rule** interface configuration commands to enable web authentication on a specific interface.

Examples	This example shows how to configure only web authentication on a switch port:
-----------------	---

```
Device# configure terminal
Device(config) ip admission name http-rule proxy http
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip access-group 101 in
Device(config-if)# ip admission rule
```

```
Device(config-if)# end
```

This example shows how to configure IEEE 802.1x authentication with web authentication as a fallback mechanism on a switch port:

```
Device# configure terminal
Device(config)# ip admission name rule2 proxy http
Device(config)# fallback profile profile1
Device(config)# ip access group 101 in
Device(config)# ip admission name rule2
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# dot1x port-control auto
Device(config-if)# dot1x fallback profile1
Device(config-if)# end
```

Related Commands	Command	Description
	dot1x fallback	Configures a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication.
	fallback profile	Creates a web authentication fallback profile.
	ip admission	Enables web authentication on a port.
	show authentication sessions interface <i>interface</i> detail	Displays information about the web authentication session status.
	show ip admission	Displays information about NAC cached entries or the NAC configuration.

ip dhcp snooping database

To configure the Dynamic Host Configuration Protocol (DHCP)-snooping database, use the **ip dhcp snooping database** command in global configuration mode. To disable the DHCP-snooping database, use the **no** form of this command.

```
no ip dhcp snooping database [ timeout | write-delay ]
```

Syntax Description	flash:url	Specifies the database URL for storing entries using flash.
	ftp:url	Specifies the database URL for storing entries using FTP.

ip dhcp snooping database

http:url	Specifies the database URL for storing entries using HTTP.
https:url	Specifies the database URL for storing entries using secure HTTP (https).
rcp:url	Specifies the database URL for storing entries using remote copy (rcp).
scp:url	Specifies the database URL for storing entries using Secure Copy (SCP).
tftp:url	Specifies the database URL for storing entries using TFTP.
timeout seconds	Specifies the abort timeout interval; valid values are from 0 to 86400 seconds.
write-delay seconds	Specifies the amount of time before writing the DHCP-snooping entries to an external server after a change is seen in the local DHCP-snooping database; valid values are from 15 to 86400 seconds.

Command Default The DHCP-snooping database is not configured.

Command Modes Global configuration

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines You must enable DHCP snooping on the interface before entering this command. Use the **ip dhcp snooping** command to enable DHCP snooping.

This example shows how to specify the database URL using TFTP:

```
Device(config)# ip dhcp snooping database tftp://10.90.90.90/snooping-rp2
```

This example shows how to specify the amount of time before writing DHCP snooping entries to an external server:

```
Device(config)# ip dhcp snooping database write-delay 15
```

ip dhcp snooping information option format remote-id

To configure the option-82 remote-ID suboption, use the **ip dhcp snooping information option format remote-id** command in global configuration mode on the switch to configure the option-82 remote-ID suboption. To configure the default remote-ID suboption, use the **no** form of this command.

```
ip dhcp snooping information option format remote-id {hostname | string string}
no ip dhcp snooping information option format remote-id {hostname | string string}
```

Syntax Description

hostname Specify the switch hostname as the remote ID.

string string Specify a remote ID, using from 1 to 63 ASCII characters (no spaces).

Command Default

The switch MAC address is the remote ID.

Command Modes

Global configuration

Command History

Release

Cisco IOS XE Everest 16.6.1

Modification

This command was introduced.

Usage Guidelines

You must globally enable DHCP snooping by using the **ip dhcp snooping** global configuration command for any DHCP snooping configuration to take effect.

When the option-82 feature is enabled, the default remote-ID suboption is the switch MAC address. This command allows you to configure either the switch hostname or a string of up to 63 ASCII characters (but no spaces) to be the remote ID.



Note

If the hostname exceeds 63 characters, it will be truncated to 63 characters in the remote-ID configuration.

This example shows how to configure the option- 82 remote-ID suboption:

```
Device(config)# ip dhcp snooping information option format remote-id hostname
```

ip dhcp snooping verify no-relay-agent-address

To disable the DHCP snooping feature from verifying that the relay agent address (giaddr) in a DHCP client message matches the client hardware address on an untrusted port, use the **ip dhcp snooping verify no-relay-agent-address** command in global configuration mode. To enable verification, use the **no** form of this command.

```
ip dhcp snooping verify no-relay-agent-address
no ip dhcp snooping verify no-relay-agent-address
```

ip http access-class

Syntax Description	This command has no arguments or keywords.	
Command Default	The DHCP snooping feature verifies that the relay-agent IP address (giaddr) field in DHCP client message on an untrusted port is 0.	
Command Modes	Global configuration	
Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.
Usage Guidelines	By default, the DHCP snooping feature verifies that the relay-agent IP address (giaddr) field in DHCP client message on an untrusted port is 0; the message is dropped if the giaddr field is not 0. Use the ip dhcp snooping verify no-relay-agent-address command to disable the verification. Use the no ip dhcp snooping verify no-relay-agent-address to reenable verification.	

This example shows how to enable verification of the giaddr in a DHCP client message:

```
Device(config)# no ip dhcp snooping verify no-relay-agent-address
```

ip http access-class

To specify the access list that should be used to restrict access to the HTTP server, use the **ip http access-class** command in global configuration mode. To remove a previously configured access list association, use the **no** form of this command.



Note The existing **ip http access-class access-list-number** command is currently supported, but is going to be deprecated. Use the **ip http access-class ipv4 { access-list-number | access-list-name }** and **ip http access-class ipv6 access-list-name** instead.

```
ip http access-class { access-list-number | ipv4 { access-list-number | access-list-name } | ipv6 access-list-name }
no ip http access-class { access-list-number | ipv4 { access-list-number | access-list-name } | ipv6 access-list-name }
```

Syntax Description	ipv4	Specifies the IPv4 access list to restrict access to the secure HTTP server.
	ipv6	Specifies the IPv6 access list to restrict access to the secure HTTP server.
	<i>access-list-number</i>	Standard IP access list number in the range 0 to 99, as configured by the access-list global configuration command.
	<i>access-list-name</i>	Name of a standard IPv4 access list, as configured by the ip access-list command.

Command Default No access list is applied to the HTTP server.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Denali 16.3.1	This command was modified. The ipv4 and ipv6 keyword were added.
Cisco IOS XE Release 3.3SE	This command was introduced.

Usage Guidelines

If this command is configured, the specified access list is assigned to the HTTP server. Before the HTTP server accepts a connection, it checks the access list. If the check fails, the HTTP server does not accept the request for a connection.

Examples

The following example shows how to define an access list as 20 and assign it to the HTTP server:

```
Device(config)# ip access-list standard 20
Device(config-std-nacl)# permit 209.165.202.130 0.0.0.255
Device(config-std-nacl)# permit 209.165.201.1 0.0.255.255
Device(config-std-nacl)# permit 209.165.200.225 0.255.255.255
Device(config-std-nacl)# exit
Device(config)# ip http access-class 20
```

The following example shows how to define an IPv4 named access list as and assign it to the HTTP server.

```
Device(config)# ip access-list standard Internet_filter
Device(config-std-nacl)# permit 1.2.3.4
Device(config-std-nacl)# exit
Device(config)# ip http access-class ipv4 Internet_filter
```

Related Commands

Command	Description
ip access-list	Assigns an ID to an access list and enters access list configuration mode.
ip http server	Enables the HTTP 1.1 server, including the Cisco web browser user interface.

ip radius source-interface

To force RADIUS to use the IP address of a specified interface for all outgoing RADIUS packets, use the **ip radius source-interface** command in global configuration mode. To prevent RADIUS from using the IP address of a specified interface for all outgoing RADIUS packets, use the no form of this command.

ip radius source-interface

ip radius source-interface *interface-name* [vrf** *vrf-name*]**
no ip radius source-interface

Syntax Description	<table border="1"> <tr> <td><i>interface-name</i></td><td>Name of the interface that RADIUS uses for all of its outgoing packets.</td></tr> <tr> <td>vrf <i>vrf-name</i></td><td>(Optional) Per virtual route forwarding (VRF) configuration.</td></tr> </table>	<i>interface-name</i>	Name of the interface that RADIUS uses for all of its outgoing packets.	vrf <i>vrf-name</i>	(Optional) Per virtual route forwarding (VRF) configuration.
<i>interface-name</i>	Name of the interface that RADIUS uses for all of its outgoing packets.				
vrf <i>vrf-name</i>	(Optional) Per virtual route forwarding (VRF) configuration.				
Command Default	No default behavior or values.				
Command Modes	Global configuration (config)				
Command History	<table border="1"> <thead> <tr> <th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td><td>This command was introduced.</td></tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				
Usage Guidelines	<p>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 <i>up</i> 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 <i>up</i> or <i>down</i> state.</p> <p>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.</p> <p>The specified interface should have a valid IP address and should be in the <i>up</i> state for a valid configuration. If the specified interface does not have a valid IP address or is in the <i>down</i> 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 <i>up</i> state.</p> <p>Use the vrf <i>vrf-name</i> 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.</p>				
Examples	<p>The following example shows how to configure RADIUS to use the IP address of interface s2 for all outgoing RADIUS packets:</p> <pre>ip radius source-interface s2</pre> <p>The following example shows how to configure RADIUS to use the IP address of interface Ethernet0 for VRF definition:</p> <pre>ip radius source-interface Ethernet0 vrf vrf1</pre>				

ip source binding

To add a static IP source binding entry, use the **ip source binding** command. Use the **no** form of this command to delete a static IP source binding entry.

```
ip source binding mac-address vlan vlan-id ip-address interface interface-id
no ip source binding mac-address vlan vlan-id ip-address interface interface-id
```

Syntax Description		
	<i>mac-address</i>	Binding MAC address.
	vlan <i>vlan-id</i>	Specifies the Layer 2 VLAN identification; valid values are from 1 to 4094.
	<i>ip-address</i>	Binding IP address.
	interface <i>interface-id</i>	ID of the physical interface.

Command Default No IP source bindings are configured.

Command Modes Global configuration.

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines You can use this command to add a static IP source binding entry only.

The **no** format deletes the corresponding IP source binding entry. It requires the exact match of all required parameter in order for the deletion to be successful. Note that each static IP binding entry is keyed by a MAC address and a VLAN number. If the command contains the existing MAC address and VLAN number, the existing binding entry is updated with the new parameters instead of creating a separate binding entry.

This example shows how to add a static IP source binding entry:

```
Device# configure terminal
Deviceconfig) ip source binding 0100.0230.0002 vlan 11 10.0.0.4 interface gigabitethernet1/0/1
```

ip verify source

To enable IP source guard on an interface, use the **ip verify source** command in interface configuration mode. To disable IP source guard, use the **no** form of this command.

```
ip verify source [mac-check] [tracking]
no ip verify source
```

ipv6 access-list

mac-check	(Optional) Enables IP source guard with MAC address verification.
tracking	(Optional) Enables IP port security to learn static IP address learning on a port.

Command Default	IP source guard is disabled.				
Command Modes	Interface configuration				
Command History	<table border="1"> <thead> <tr> <th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td><td>This command was introduced.</td></tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				
Usage Guidelines	<p>To enable IP source guard with source IP address filtering, use the ip verify source interface configuration command.</p> <p>To enable IP source guard with source IP address filtering and MAC address verification, use the ip verify source mac-check interface configuration command.</p>				

Examples	This example shows how to enable IP source guard with source IP address filtering on an interface:
	<pre>Device(config)# interface gigabitethernet1/0/1 Device(config-if)# ip verify source</pre>

This example shows how to enable IP source guard with MAC address verification:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip verify source mac-check
```

You can verify your settings by entering the **show ip verify source** privileged EXEC command.

ipv6 access-list

To define an IPv6 access list and to place the device in IPv6 access list configuration mode, use the **ipv6 access-list** command in global configuration mode. To remove the access list, use the **no** form of this command.

```
ipv6 access-list access-list-name | match-local-traffic | log-update threshold threshold-in-msgs | role-based list-name
noipv6 access-list access-list-name | client permit-control-packets | log-update threshold | role-based list-name
```

Syntax Description	ipv6 <i>access-list-name</i> <p><i>access-list-name</i> - Name of the IPv6 access list. Names cannot contain a space or quotation mark, or begin with a numeric.</p>
---------------------------	---

match-local-traffic	Enables matching for locally-generated traffic.
log-update threshold <i>threshold-in-msgs</i>	Determines how syslog messages are generated after the initial packet match. <i>threshold-in-msgs-</i> Number of packets generated.
role-based <i>list-name</i>	Creates a role-based IPv6 ACL.

Command Default No IPv6 access list is defined.

Command Modes Global configuration

Command History	Release	Modification
		This command was reintroduced. This command was not supported in and

Usage Guidelines IPv6 ACLs are defined by using the **ipv6 access-list** command in global configuration mode and their permit and deny conditions are set by using the **deny** and **permit** commands in IPv6 access list configuration mode. Configuring the **ipv6 access-list** command places the device in IPv6 access list configuration mode—the device prompt changes to Device(config-ipv6-acl)#. From IPv6 access list configuration mode, permit and deny conditions can be set for the defined IPv6 ACL.



Note IPv6 ACLs are defined by a unique name (IPv6 does not support numbered ACLs). An IPv4 ACL and an IPv6 ACL cannot share the same name.

IPv6 is automatically configured as the protocol type in **permit any any** and **deny any any** statements that are translated from global configuration mode to IPv6 access list configuration mode.

Every IPv6 ACL has implicit **permit icmp any any nd-na**, **permit icmp any any nd-ns**, and **deny ipv6 any any** statements as its last match conditions. (The former two match conditions allow for ICMPv6 neighbor discovery.) An IPv6 ACL must contain at least one entry for the implicit **deny ipv6 any any** statement to take effect. The IPv6 neighbor discovery process makes use of the IPv6 network layer service; therefore, by default, IPv6 ACLs implicitly allow IPv6 neighbor discovery packets to be sent and received on an interface. In IPv4, the Address Resolution Protocol (ARP), which is equivalent to the IPv6 neighbor discovery process, makes use of a separate data link layer protocol; therefore, by default, IPv4 ACLs implicitly allow ARP packets to be sent and received on an interface.

Use the **ipv6 traffic-filter** interface configuration command with the *access-list-name* argument to apply an IPv6 ACL to an IPv6 interface. Use the **ipv6 access-class** line configuration command with the *access-list-name* argument to apply an IPv6 ACL to incoming and outgoing IPv6 virtual terminal connections to and from the device.

An IPv6 ACL applied to an interface with the **ipv6 traffic-filter** command filters traffic that is forwarded, not originated, by the device.

Examples

The example configures the IPv6 ACL list named list1 and places the device in IPv6 access list configuration mode.

ipv6 snooping policy

```
Device(config)# ipv6 access-list list1
Device(config-ipv6-acl)#

```

The following example configures the IPv6 ACL named list2 and applies the ACL to outbound traffic on Ethernet interface 0. Specifically, the first ACL entry keeps all packets from the network FEC0:0:0:2::/64 (packets that have the site-local prefix FEC0:0:0:2 as the first 64 bits of their source IPv6 address) from exiting out of Ethernet interface 0. The second entry in the ACL permits all other traffic to exit out of Ethernet interface 0. The second entry is necessary because an implicit deny all condition is at the end of each IPv6 ACL.

```
Device(config)# ipv6 access-list list2 deny FEC0:0:0:2::/64 any
Device(config)# ipv6 access-list list2 permit any any
Device(config)# interface ethernet 0
Device(config-if)# ipv6 traffic-filter list2 out

```

ipv6 snooping policy



Note All existing IPv6 Snooping commands (prior to) now have corresponding SISF-based device-tracking commands that allow you to apply your configuration to both IPv4 and IPv6 address families. For more information, see [device-tracking policy](#)

To configure an IPv6 snooping policy and enter IPv6 snooping configuration mode, use the **ipv6 snooping policy** command in global configuration mode. To delete an IPv6 snooping policy, use the **no** form of this command.

ipv6 snooping policy *snooping-policy*
no ipv6 snooping policy *snooping-policy*

Syntax Description	<i>snooping-policy</i>	User-defined name of the snooping policy. The policy name can be a symbolic string (such as Engineering) or an integer (such as 0).
Command Default	An IPv6 snooping policy is not configured.	
Command Modes	Global configuration	
Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	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: <ul style="list-style-type: none"> The device-role command specifies the role of the device attached to the port. The limit address-count <i>maximum</i> command limits the number of IPv6 addresses allowed to be used on the port. 	

- The **protocol** command specifies that addresses should be gleaned with Dynamic Host Configuration Protocol (DHCP) or Neighbor Discovery Protocol (NDP).
- The **security-level** command specifies the level of security enforced.
- The **tracking** command overrides the default tracking policy on a port.
- The **trusted-port** command configures a port to become a trusted port; that is, limited or no verification is performed when messages are received.

This example shows how to configure an IPv6 snooping policy:

```
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping) #
```

key chain macsec

To configure a MACsec key chain name on a device interface to fetch a Pre Shared Key (PSK), use the **key chain macsec** command in global configuration mode. To disable it, use the **no** form of this command.

key chain *name* macsec {description | key | exit}

Syntax Description

<i>name</i>	Name of a key chain to be used to get keys.
description	Provides description of the MACsec key chain.
key	Configure a MACsec key.
exit	Exits from the MACsec key-chain configuration mode.
no	Negates the command or sets the default values.

Command Default

key chain macsec is disabled.

Command Modes

Global configuration

Command History

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

This example shows how to configure MACsec key chain to fetch a 128-bit Pre Shared Key (PSK):

```
Switch#configure terminal
Switch(config)#key chain kc1 macsec
Switch(config-keychain-macsec)#key 1000
Switch(config-keychain-macsec)#cryptographic-algorithm aes-128-cmac
Switch(config-keychain-macsec-key)# key-string fb63e0269e2768c49bab8ee9a5c2258f
Switch(config-keychain-macsec-key)#end
Switch#
```

This example shows how to configure MACsec key chain to fetch a 256-bit Pre Shared Key (PSK):

```
Switch#configure terminal
Switch(config)#key chain kcl macsec
Switch(config-keychain-macsec)#key 2000
Switch(config-keychain-macsec)#cryptographic-algorithm aes-256-cmac
Switch(config-keychain-macsec-key)# key-string
c865632acb269022447c417504a1bf5db1c296449b52627ba01f2ba2574c2878
Switch(config-keychain-macsec-key)#end
Switch#
```

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	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.	
Release	Modification					
Cisco IOS XE Everest 16.6.1	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.

Command	Description
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 ND inspection policy configuration
 IPv6 snooping configuration

Command History	Release	Modification
Cisco IOS XE Everest 16.6.1		This command was introduced.

Usage Guidelines The **limit address-count** command limits the number of IPv6 addresses allowed to be used on the port on which the policy is applied. Limiting the number of IPv6 addresses on a port helps limit the binding table size. The range is from 1 to 10000.

This example shows how to define an NDP policy name as policy1, place the switch in NDP inspection policy configuration mode, and limit the number of IPv6 addresses allowed on the port to 25:

```
Device(config)# ipv6 nd inspection policy policy1
Device(config-nd-inspection)# limit address-count 25
```

This example shows how to define an IPv6 snooping policy name as policy1, place the switch in IPv6 snooping policy configuration mode, and limit the number of IPv6 addresses allowed on the port to 25:

```
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# limit address-count 25
```

mab request format attribute 32

To enable VLAN ID-based MAC authentication on a switch, use the **mab request format attribute 32 vlan access-vlan** command in global configuration mode. To return to the default setting, use the **no** form of this command.

```
mab request format attribute 32 vlan access-vlan
no mab request format attribute 32 vlan access-vlan
```

Syntax Description	This command has no arguments or keywords.	
Command Default	VLAN-ID based MAC authentication is disabled.	
Command Modes	Global configuration	
Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.
Usage Guidelines	<p>Use this command to allow a RADIUS server to authenticate a new user based on the host MAC address and VLAN.</p> <p>Use this feature on networks with the Microsoft IAS RADIUS server. The Cisco ACS ignores this command.</p>	

This example shows how to enable VLAN-ID based MAC authentication on a switch:

```
Device(config)# mab request format attribute 32 vlan access-vlan
```

Related Commands	Command	Description
	authentication event	Sets the action for specific authentication events.
	authentication fallback	Configures a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication.
	authentication host-mode	Sets the authorization manager mode on a port.
	authentication open	Enables or disables open access on a port.
	authentication order	Sets the order of authentication methods used on a port.
	authentication periodic	Enables or disables reauthentication on a port.
	authentication port-control	Enables manual control of the port authorization state.
	authentication priority	Adds an authentication method to the port-priority list.

Command	Description
authentication timer	Configures the timeout and reauthentication parameters for an 802.1x-enabled port.
authentication violation	Configures the violation modes that occur when a new device connects to a port or when a new device connects to a port with the maximum number of devices already connected to that port.
mab	Enables MAC-based authentication on a port.
mab eap	Configures a port to use the Extensible Authentication Protocol (EAP).
show authentication	Displays information about authentication manager events on the switch.

macsec-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 | gcm-aes-256}
no macsec-cipher-suite {gcm-aes-128 | gcm-aes-256}
```

Syntax Description

gcm-aes-128 Configures cipher suite for deriving SAK with 128-bit encryption.

gcm-aes-256 Configures cipher suite for deriving SAK with 256-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 Everest 16.6.1	This command was introduced.

Usage Guidelines

If the device supports both GCM-AES-128 and GCM-AES-256 ciphers, it is highly recommended to define and use a user-defined MKA policy to include both or only 256 bits cipher, based on your requirements..

Examples

The following example shows how to configure MACsec cipher suite for deriving SAK with 256-bit encryption:

```
Device> enable
Device# configure terminal
Device(config)# mka policy 2
Device(config-mka-policy)# macsec-cipher-suite gcm-aes-256
```

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 MKA MACsec configuration on the uplink interfaces, use the **macsec network-link** command on the interface. To disable it, use the **no** form of this command.

macsec network-link

Syntax Description	macsec network-link Enables MKA MACsec configuration on device interfaces using EAP-TLS authentication protocol.	
Command Default	macsec network-link is disabled.	
Command Modes	Interface configuration	
Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

This example shows how to configure MACsec MKA on an interface using the EAP-TLS authentication protocol:

```
Switch#configure terminal
Switch(config)# int G1/0/20
Switch(config-if)# macsec network-link
Switch(config-if)# end
Switch#
```

match (access-map configuration)

To set the VLAN map to match packets against one or more access lists, use the **match** command in access-map configuration mode on the switch stack or on a standalone switch. To remove the match parameters, use the **no** form of this command.

```
match {ip address {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

Command History

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines

You enter access-map configuration mode by using the **vlan access-map** global configuration command.

You must enter one access list name or number; others are optional. You can match packets against one or more access lists. Matching any of the lists counts as a match of the entry.

In access-map configuration mode, use the **match** command to define the match conditions for a VLAN map applied to a VLAN. Use the **action** command to set the action that occurs when the packet matches the conditions.

Packets are matched only against access lists of the same protocol type; IP packets are matched against IP access lists, IPv6 packets are matched against IPv6 access lists, and all other packets are matched against MAC access lists.

IP, IPv6, and MAC addresses can be specified for the same map entry.

This example shows how to define and apply a VLAN access map vmap4 to VLANs 5 and 6 that will cause the interface to drop an IP packet if the packet matches the conditions defined in access list al2:

```
Device(config)# vlan access-map vmap4
Device(config-access-map)# match ip address al2
Device(config-access-map)# action drop
```

mka pre-shared-key

```
Device(config-access-map) # exit
Device(config) # vlan filter vmap4 vlan-list 5-6
```

You can verify your settings by entering the **show vlan access-map** privileged EXEC command.

mka pre-shared-key

To configure MKA MACsec on a device interface using a Pre Shared Key (PSK), use the **mka pre-shared-key key-chain *key-chain name*** command in global configuration mode. To disable it, use the **no** form of this command.

mka pre-shared-key key-chain *key-chain-name*

Syntax Description	mka pre-shared-key key-chain Enables MACsec MKA configuration on device interfaces using a PSK.	
Command Default	mka pre-shared-key is disabled.	
Command Modes	Interface configuration	
Command History		
Release	Modification	
Cisco IOS XE Denali 16.3.1		This command was introduced.

This example shows how to configure MKA MACsec on an interface using a PSK:

```
Switch#
Switch(config) # int G1/0/20
Switch(config-if) # mka pre-shared-key key-chain kc1
Switch(config-if) # end
Switch#
```

mka suppress syslogs sak-rekey

To suppress MACsec Key Agreement (MKA) secure association key (SAK) rekey messages during logging, use the **mka suppress syslogs sak-rekey** command in global configuration mode. To enable MKA SAK rekey message logging, use the **no** form of this command.

mka suppress syslogs sak-rekey
no mka suppress syslogs sak-rekey

This command has no arguments or keywords.

Command Default	All MKA SAK syslog messages are displayed on the console.
Command Modes	Global configuration (config)

Command History	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 how to suppress MKA SAK syslog logging:

```
Device> enable
Device# configure terminal
Device(config)# mka suppress syslogs sak-rekey
```

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 Everest 16.6.1	This command was introduced.

Usage Guidelines	This command filters details, such as anticipated success, from authentication system messages. Failure messages are not filtered.
------------------	--

To filter verbose authentication system messages:

```
Device(config)# authentication logging verbose
```

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

Related Commands	Command	Description
	authentication logging verbose	Filters details from authentication system messages.

dot1x logging verbose

Command	Description
dot1x logging verbose	Filters details from 802.1x system messages.
mab logging verbose	Filters details from MAC authentication bypass (MAB) system messages.

dot1x logging verbose

To filter detailed information from 802.1x system messages, use the **dot1x logging verbose** command in global configuration mode on the switch stack or on a standalone switch.

```
dot1x logging verbose
no dot1x logging verbose
```

Syntax Description	This command has no arguments or keywords.	
Command Default	Detailed logging of system messages is not enabled.	
Command Modes	Global configuration (config)	
Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines This command filters details, such as anticipated success, from 802.1x system messages. Failure messages are not filtered.

To filter verbose 802.1x system messages:

```
Device(config)# dot1x logging verbose
```

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

Related Commands	Command	Description
	authentication logging verbose	Filters details from authentication system messages.
	dot1x logging verbose	Filters details from 802.1x system messages.
	mab logging verbose	Filters details from MAC authentication bypass (MAB) system messages.

mab logging verbose

To filter detailed information from MAC authentication bypass (MAB) system messages, use the **mab logging verbose** command in global configuration mode on the switch stack or on a standalone switch.

```
mab logging verbose
no mab logging verbose
```

Syntax Description This command has no arguments or keywords.

Command Default Detailed logging of system messages is not enabled.

Command Modes Global configuration (config)

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines This command filters details, such as anticipated success, from MAC authentication bypass (MAB) system messages. Failure messages are not filtered.

To filter verbose MAB system messages:

```
Device(config)# mab logging verbose
```

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

Related Commands	Command	Description
	authentication logging verbose	Filters details from authentication system messages.
	dot1x logging verbose	Filters details from 802.1x system messages.
	mab logging verbose	Filters details from MAC authentication bypass (MAB) system messages.

permit (MAC access-list configuration)

To allow non-IP traffic to be forwarded if the conditions are matched, use the **permit** MAC access-list configuration command on the switch stack or on a standalone switch. To remove a permit condition from the extended MAC access list, use the **no** form of this command.

```
{permit {any | hostsrc-MAC-addr | src-MAC-addr mask} {any | hostdst-MAC-addr | dst-MAC-addr mask} [type mask | aarp | amber | appletalk | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000 | etype-8042 | lat | lave-sca | lsapsap mask | mop-console | mop-dump | msdos | mumps | netbios | vines-echo | vines-ip | xns-idp] [coscos]}
```

permit (MAC access-list configuration)

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** | **lavr-sca** | **lsap lsap mask** | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** | **vines-ip** | **xns-idp**] [**coscos**]**

Syntax Description		
any		Denies any source or destination MAC address.
host <i>src-MAC-addr</i> <i>src-MAC-addr mask</i>		Specifies a host MAC address and optional subnet mask. If the source address for a packet matches the defined address, non-IP traffic from that address is denied.
host <i>dst-MAC-addr</i> <i>dst-MAC-addr mask</i>		Specifies a destination MAC address and optional subnet mask. If the destination address for a packet matches the defined address, non-IP traffic to that address is denied.
<i>type mask</i>		(Optional) Specifies the EtherType number of a packet with Ethernet II or SNAP encapsulation to identify the protocol of the packet. <ul style="list-style-type: none"> • <i>type</i> is 0 to 65535, specified in hexadecimal. • <i>mask</i> is a mask of don't care bits applied to the EtherType before testing for a match.
aarp		(Optional) Specifies EtherType AppleTalk Address Resolution Protocol that maps a data-link address to a network address.
amber		(Optional) Specifies EtherType DEC-Amber.
appletalk		(Optional) Specifies EtherType AppleTalk/EtherTalk.
dec-spanning		(Optional) Specifies EtherType Digital Equipment Corporation (DEC) spanning tree.
decnet-iv		(Optional) Specifies EtherType DECnet Phase IV protocol.
diagnostic		(Optional) Specifies EtherType DEC-Diagnostic.
dsm		(Optional) Specifies EtherType DEC-DSM.
etype-6000		(Optional) Specifies EtherType 0x6000.
etype-8042		(Optional) Specifies EtherType 0x8042.
lat		(Optional) Specifies EtherType DEC-LAT.
lavr-sca		(Optional) Specifies EtherType DEC-LAVC-SCA.

lsap <i>lsap-number mask</i>	(Optional) Specifies the LSAP number (0 to 65535) of a packet with 802.2 encapsulation to identify the protocol of the packet. The <i>mask</i> is a mask of don't care bits applied to the LSAP number before testing for a match.
mop-console	(Optional) Specifies EtherType DEC-MOP Remote Console.
mop-dump	(Optional) Specifies EtherType DEC-MOP Dump.
msdos	(Optional) Specifies EtherType DEC-MSDOS.
mumps	(Optional) Specifies EtherType DEC-MUMPS.
netbios	(Optional) Specifies EtherType DEC- Network Basic Input/Output System (NetBIOS).
vines-echo	(Optional) Specifies EtherType Virtual Integrated Network Service (VINES) Echo from Banyan Systems.
vines-ip	(Optional) Specifies EtherType VINES IP.
xns-idp	(Optional) Specifies EtherType Xerox Network Systems (XNS) protocol suite.
cos <i>cos</i>	(Optional) Specifies an arbitrary class of service (CoS) number from 0 to 7 to set priority. Filtering on CoS can be performed only in hardware. A warning message appears if the cos option is configured.

Command Default This command has no defaults. However, the default action for a MAC-named ACL is to deny.

Command Modes Mac-access list configuration

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	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 **Isap lsap mask** keywords, depending on the type of IPX encapsulation being used. Filter criteria for IPX encapsulation types as specified in Novell terminology and Cisco IOS terminology are listed in the following table.

Table 164: IPX Filtering Criteria

IPX Encapsulation Type		Filter Criterion
Cisco IOS Name	Novell Name	
arpa	Ethernet II	EtherType 0x8137
snap	Ethernet-snap	EtherType 0x8137
sap	Ethernet 802.2	LSAP 0xE0E0
novell-ether	Ethernet 802.3	LSAP 0xFFFF

This example shows how to define the MAC-named extended access list to allow NetBIOS traffic from any source to MAC address 00c0.00a0.03fa. Traffic matching this list is allowed.

```
Device(config-ext-macl) # permit any host 00c0.00a0.03fa netbios
```

This example shows how to remove the permit condition from the MAC-named extended access list:

```
Device(config-ext-macl) # no permit any 00c0.00a0.03fa 0000.0000.0000 netbios
```

This example permits all packets with EtherType 0x4321:

```
Device(config-ext-macl) # permit any any 0x4321 0
```

You can verify your settings by entering the **show access-lists** privileged EXEC command.

Related Commands

Command	Description
deny	Denies from the MAC access-list configuration. Denies non-IP traffic to be forwarded if conditions are matched.
mac access-list extended	Creates an access list based on MAC addresses for non-IP traffic.
show access-lists	Displays access control lists configured on a switch.

propagate sgt (cts manual)

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

propagate sgt**Syntax Description**

This command has no arguments or keywords.

Command Default

SGT processing propagation is enabled.

Command Modes

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

Command History

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

Usage Guidelines

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

Examples

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

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

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

```
Switch#show cts interface brief
Global Dot1x feature is Disabled
Interface GigabitEthernet0:
    CTS is enabled, mode:      MANUAL
    IFC state:                OPEN
    Authentication Status:    NOT APPLICABLE
    Peer identity:            "unknown"
    Peer's advertised capabilities: ""
    Authorization Status:    NOT APPLICABLE
    SAP Status:               NOT APPLICABLE
    Propagate SGT:            Disabled
    Cache Info:
        Cache applied to link : NONE
```

Related Commands

Command	Description
cts manual	Enables an interface for CTS.
show cts interface	Displays Cisco TrustSec states and statistics per interface.

protocol (IPv6 snooping)

To specify that addresses should be gleaned with Dynamic Host Configuration Protocol (DHCP) or Neighbor Discovery Protocol (NDP), or to associate the protocol with an IPv6 prefix list, use the **protocol** command. To disable address gleaning with DHCP or NDP, use the **no** form of the command.

```
protocol {dhcp | ndp}
no protocol {dhcp | ndp}
```

Syntax Description	dhcp Specifies that addresses should be gleaned in Dynamic Host Configuration Protocol (DHCP) packets. ndp Specifies that addresses should be gleaned in Neighbor Discovery Protocol (NDP) packets.				
Command Default	Snooping and recovery are attempted using both DHCP and NDP.				
Command Modes	IPv6 snooping configuration mode				
Command History	<table border="1"> <thead> <tr> <th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td><td>This command was introduced.</td></tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	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. <ul style="list-style-type: none"> Using the no protocol {dhcp ndp} command indicates that a protocol will not be used for snooping or gleaning. If the no protocol dhcp command is used, DHCP can still be used for binding table recovery. Data glean can recover with DHCP and NDP, though destination guard will only recovery through DHCP. 				

This example shows how to define an IPv6 snooping policy name as policy1, place the switch in IPv6 snooping policy configuration mode, and configure the port to use DHCP to glean addresses:

```
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# protocol dhcp
```

radius server



Note Starting from Cisco IOS 15.2(5)E release, the **radius server** command replaces the **radius-server host** command, being used in releases prior to Cisco IOS Release 15.2(5)E. The old command has been deprecated.

Use the **radius server** configuration sub-mode command on the switch stack or on a standalone switch to configure the RADIUS server parameters, including the RADIUS accounting and authentication. Use the **no** form of this command to return to the default settings.

```
radius server name
address {ipv4 | ipv6} ip{address / hostname} auth-port udp-port acct-port udp-port
key string
automate tester name | retransmit value | timeout seconds
no radius server name
```

Syntax Description

address { ipv4 ipv6 } <i>ip{address / hostname}</i>	Specify the IP address of the RADIUS server.
auth-port <i>udp-port</i>	(Optional) Specify the UDP port for the RADIUS authentication server. The range is from 0 to 65536.
acct-port <i>udp-port</i>	(Optional) Specify the UDP port for the RADIUS accounting server. The range is from 0 to 65536.
key <i>string</i>	(Optional) Specify the authentication and encryption key for all RADIUS communication between the switch and the RADIUS daemon.
Note	The key is a text string that must match the encryption key used on the RADIUS server. Always configure the key as the last item in this command. Leading spaces are ignored, but spaces within and at the end of the key are used. If there are spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key.
automate tester <i>name</i>	(Optional) Enable automatic server testing of the RADIUS server status, and specify the username to be used.
retransmit <i>value</i>	(Optional) Specifies the number of times a RADIUS request is resent when the server is not responding or responding slowly. The range is 1 to 100. This setting overrides the radius-server retransmit global configuration command setting.
timeout <i>seconds</i>	(Optional) Specifies the time interval that the Switch waits for the RADIUS server to reply before sending a request again. The range is 1 to 1000. This setting overrides the radius-server timeout global configuration command setting.
no radius server <i>name</i>	Returns to the default settings

Command Default

- The UDP port for the RADIUS accounting server is 1646.
- The UDP port for the RADIUS authentication server is 1645.
- Automatic server testing is disabled.
- The timeout is 60 minutes (1 hour).
- When the automatic testing is enabled, testing occurs on the accounting and authentication UDP ports.

sak-rekey

- The authentication and encryption key (string) is not configured.

Command Modes	Radius server sub-mode configuration
----------------------	--------------------------------------

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced to replace the radius-server host command.

Usage Guidelines	<ul style="list-style-type: none"> We recommend that you configure the UDP port for the RADIUS accounting server and the UDP port for the RADIUS authentication server to non-default values. You can configure the authentication and encryption key by using the key string sub-mode configuration command. Always configure the key as the last item in this command. Use the automate-tester name keywords to enable automatic server testing of the RADIUS server status and to specify the username to be used.
-------------------------	--

This example shows how to configure 1645 as the UDP port for the authentication server and 1646 as the UDP port for the accounting server, and configure a key string:

```
Device(config)# radius server ISE
Device(config-radius-server)# address ipv4 10.1.1 auth-port 1645 acct-port 1646
Device(config-radius-server)# key cisco123
```

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	<table> <tr> <td>interval</td><td>SAK rekey interval in seconds.</td></tr> <tr> <td><i>time-interval</i></td><td>The range is from 30 to 65535, and the default is 0.</td></tr> <tr> <td>on-live-peer-loss</td><td>Peer loss from the live membership.</td></tr> </table>	interval	SAK rekey interval in seconds.	<i>time-interval</i>	The range is from 30 to 65535, and the default is 0.	on-live-peer-loss	Peer loss from the live membership.
interval	SAK rekey interval in seconds.						
<i>time-interval</i>	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 16.8.1a	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.

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.).
----------------------	---

sap mode-list (cts manual)

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)

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

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

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

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

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

Examples

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

```
Switch# configure terminal
Switch(config)# interface gigabitethernet 2/1
Switch(config-if)# cts manual
Switch(config-if-cts-manual)# sap pmk 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.

security level (IPv6 snooping)

To specify the level of security enforced, use the **security-level** command in IPv6 snooping policy configuration mode.

security level {glean | guard | inspect}

Syntax Description	glean Extracts addresses from the messages and installs them into the binding table without performing any verification.				
	guard Performs both glean and inspect. Additionally, RA and DHCP server messages are rejected unless they are received on a trusted port or another policy authorizes them.				
	inspect Validates messages for consistency and conformance; in particular, address ownership is enforced. Invalid messages are dropped.				
Command Default	The default security level is guard.				
Command Modes	IPv6 snooping configuration				
Command History	<table border="1"> <thead> <tr> <th style="text-align: left;">Release</th> <th style="text-align: right;">Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td> <td style="text-align: right;">This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				

This example shows how to define an IPv6 snooping policy name as policy1, place the device in IPv6 snooping configuration mode, and configure the security level as inspect:

```
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# security-level inspect
```

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)

server-private (RADIUS)

Command History	Release	Modification
	Cisco IOS XE Fuji 16.9.1	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	<i>ip-address</i>	IP address of the private RADIUS server host.
--------------------	-------------------	---

auth-port <i>port-number</i>	(Optional) User Datagram Protocol (UDP) destination port for authentication requests. The default value is 1645.
acct-port <i>port-number</i>	(Optional) UDP destination port for accounting requests. The default value is 1646.
non-standard	(Optional) RADIUS server is using vendor-proprietary RADIUS attributes.
timeout <i>seconds</i>	(Optional) Time interval (in seconds) that the 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 <i>retries</i>	(Optional) Number of times a RADIUS request is resent to a server, if that server is not responding or responding slowly. This setting overrides the global setting of the radius-server retransmit command.
key <i>string</i>	(Optional) Authentication and encryption key used between the 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 <i>string</i> can be 0 (specifies that an unencrypted key follows), 6 (specifies that an advanced encryption scheme [AES] encrypted key follows), 7 (specifies that a hidden key follows), or a line specifying the unencrypted (clear-text) server key.

Command Default If server-private parameters are not specified, global configurations will be used; if global configurations are not specified, default values will be used.

Command Modes RADIUS server-group configuration (config-sg-radius)

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines Use the **server-private** command to associate a particular private server with a defined server group. To prevent possible overlapping of private addresses between virtual route forwarding (VRF) instances, private servers (servers with private addresses) can be defined within the server group and remain hidden from other groups, while the servers in the global pool (default "radius" server group) can still be referred to by IP addresses and port numbers. Thus, the list of servers in server groups includes references to the hosts in the global configuration and the definitions of private servers.

**Note**

- If the **radius-server directed-request** command is configured, then a private RADIUS server cannot be used as the group server by configuring the **server-private** (RADIUS) command.
- Creating or updating AAA server statistics record for private RADIUS servers are not supported. If private RADIUS servers are used, then error messages and tracebacks will be encountered, but these error messages or tracebacks do not have any impact on the AAA RADIUS functionality. To avoid these error messages and tracebacks, configure public RADIUS server instead of private RADIUS server.

show aaa clients

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.

show aaa clients

To show AAA client statistics, use the **show aaa clients** command.

show aaa clients [detailed]

Syntax Description

detailed (Optional) Shows detailed AAA client statistics.

Command Modes

User EXEC

Command History

Release

Modification

Cisco IOS XE Everest 16.6.1

This command was introduced.

This is an example of output from the **show aaa clients** command:

```
Device# show aaa clients
Dropped request packets: 0
```

show aaa command handler

To show AAA command handler statistics, use the **show aaa command handler** command.

show aaa command handler

Syntax Description	This command has no arguments or keywords.	
Command Modes	User EXEC	
Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

This is an example of output from the **show aaa command handler** command:

```
Device# show aaa command handler

AAA Command Handler Statistics:
  account-logon: 0, account-logoff: 0
  account-query: 0, pod: 0
  service-logon: 0, service-logoff: 0
  user-profile-push: 0, session-state-log: 0
  reauthenticate: 0, bounce-host-port: 0
  disable-host-port: 0, update-rbacl: 0
  update-sgt: 0, update-cts-policies: 0
  invalid commands: 0
  async message not sent: 0
```

show aaa local

To show AAA local method options, use the **show aaa local** command.

show aaa local {netuser {name | all} | statistics | user lockout}

Syntax Description	netuser	Specifies the AAA local network or guest user database.
	<i>name</i>	Network user name.
	all	Specifies the network and guest user information.
	statistics	Displays statistics for local authentication.
	user lockout	Specifies the AAA local locked-out user.

Command Modes	User EXEC
----------------------	-----------

show aaa servers

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	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 Everest 16.6.1	This command was introduced.

Examples

The following is a sample output from the **show aaa servers** command:

```
Device# show aaa servers

RADIUS: id 1, priority 1, host 172.20.128.2, auth-port 1645, acct-port 1646
State: current UP, duration 9s, previous duration 0s
Dead: total time 0s, count 0
Quarantined: No
Authen: request 0, timeouts 0, failover 0, retransmission 0
Response: accept 0, reject 0, challenge 0
Response: unexpected 0, server error 0, incorrect 0, time 0ms
Transaction: success 0, failure 0
Throttled: transaction 0, timeout 0, failure 0
Author: request 0, timeouts 0, failover 0, retransmission 0
Response: accept 0, reject 0, challenge 0
Response: unexpected 0, server error 0, incorrect 0, time 0ms
Transaction: success 0, failure 0
Throttled: transaction 0, timeout 0, failure 0
Account: request 0, timeouts 0, failover 0, retransmission 0
Request: start 0, interim 0, stop 0
Response: start 0, interim 0, stop 0
Response: unexpected 0, server error 0, incorrect 0, time 0ms
Transaction: success 0, failure 0
Throttled: transaction 0, timeout 0, failure 0
Elapsed time since counters last cleared: 0m
Estimated Outstanding Access Transactions: 0
Estimated Outstanding Accounting Transactions: 0
Estimated Throttled Access Transactions: 0
Estimated Throttled Accounting Transactions: 0
Maximum Throttled Transactions: access 0, accounting 0
```

show aaa sessions

To show AAA sessions as seen by the AAA Session MIB, use the **show aaa sessions** command.

show aaa sessions

Syntax Description	This command has no arguments or keywords.	
Command Modes	User EXEC	
Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

This is an example of output from the **show aaa sessions** command:

```
Device# show aaa sessions
```

show authentication brief

```
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 <i>switch-number</i> 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 Everest 16.6.1	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 165: 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.

show authentication sessions

Field	Description
Fg	Flag indicates the current status. The valid values are: <ul style="list-style-type: none"> • 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	
Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	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 166: Authentication Method States

State	Description
Not run	The method has not run for this session.
Running	The method is running for this session.
Failed over	The method has failed and the next method is expected to provide a result.
Success	The method has provided a successful authentication result for the session.
Authc Failed	The method has provided a failed authentication result for the session.

This table shows the possible authentication methods.

Table 167: Authentication Method States

State	Description
dot1x	802.1X
mab	MAC authentication bypass
webauth	web authentication

The following example shows how to display all authentication sessions on the switch:

```
Device# show authentication sessions
Interface      MAC Address      Method      Domain      Status      Session ID
Gi1/0/48       0015.63b0.f676   dot1x      DATA        Authz Success  0A3462B1000000102983C05C
Gi1/0/5        000f.23c4.a401   mab        DATA        Authz Success  0A3462B10000000D24F80B58
Gi1/0/5        0014.bf5d.d26d   dot1x      DATA        Authz Success  0A3462B10000000E29811B94
```

The following example shows how to display all authentication sessions on an interface:

```
Device# show authentication sessions interface gigabitethernet2/0/47
      Interface: GigabitEthernet2/0/47
      MAC Address: Unknown
      IP Address: Unknown
```

show cts interface

```

        Status: Authz Success
        Domain: DATA
        Oper host mode: multi-host
        Oper control dir: both
        Authorized By: Guest Vlan
        Vlan Policy: 20
        Session timeout: N/A
        Idle timeout: N/A
        Common Session ID: 0A3462C80000000000002763C
        Acct Session ID: 0x00000002
        Handle: 0x25000000
Runnable methods list:
    Method      State
    mab         Failed over
    dot1x       Failed over
-----
        Interface: GigabitEthernet2/0/47
        MAC Address: 0005.5e7c.da05
        IP Address: Unknown
        User-Name: 00055e7cd05
        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: 0A3462C80000000010002A238
        Acct Session ID: 0x00000003
        Handle: 0x91000001
Runnable methods list:
    Method      State
    mab         Authc Success
    dot1x       Not run

```

show cts interface

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

show cts interface [{type slot/port | brief | summary}]

Syntax Description	<table border="1"> <tr> <td>type slot/port</td><td>(Optional) Specifies an interface type and slot or port number. A verbose output for this interface is returned.</td></tr> <tr> <td>brief</td><td>(Optional) Displays abbreviated status for all CTS interfaces.</td></tr> <tr> <td>summary</td><td>(Optional) Displays a tabular summary of all CTS interfaces with 4 or 5 key status fields for each interface.</td></tr> </table>	type slot/port	(Optional) Specifies an interface type and slot or port number. A verbose output for this interface is returned.	brief	(Optional) Displays abbreviated status for all CTS interfaces.	summary	(Optional) Displays a tabular summary of all CTS interfaces with 4 or 5 key status fields for each interface.
type slot/port	(Optional) Specifies an interface type and slot or port number. A verbose output for this interface is returned.						
brief	(Optional) Displays abbreviated status for all CTS interfaces.						
summary	(Optional) Displays a tabular summary of all CTS interfaces with 4 or 5 key status fields for each interface.						

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

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

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was modified with additional options.
	Cisco IOS XE Denali 16.2.1	This command was introduced.

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

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

```

Switch# show cts interface

Global Dot1x feature is Disabled
Interface GigabitEthernet0/1/0:
    CTS is enabled, mode: MANUAL
    IFC state: OPEN
    Interface Active for 00:00:18.232
    Authentication Status: NOT APPLICABLE
        Peer identity: "unknown"
        Peer's advertised capabilities: ""
    Authorization Status: NOT APPLICABLE
    SAP Status: NOT APPLICABLE
    Configured pairwise ciphers:
        gcm-encrypt
        null

    Replay protection: enabled
    Replay protection mode: STRICT

    Selected cipher:

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

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

```

show cts role-based permissions

```
unknown sa dropped:      0
unknown sa bypassed:     0
```

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

```
Device# show cts interface brief

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

Related Commands	Command	Description
	cts manual	Enables an interface for CTS.
	propagate sgt (cts manual)	Enables Security Group Tag (SGT) propagation at Layer 2 on Cisco TrustSec Security (CTS) interfaces.
	sap mode-list (cts manual)	Manually specifies the PMK and the SAP authentication and encryption modes to negotiate MACsec link encryption between two interfaces.

show cts role-based permissions

To display the role-based (security group) access control permission list, use the **show cts role-based permissions** command in privileged EXEC mode.

```
show cts role-based permissions [{default [{details | ipv4 [{details}]}] | from [{sgt [{ipv4 | to [{sgt | unknown}]} [{details | ipv4 [{details}]}]} | unknown]} | ipv4 | to [{sgt | unknown}] [{ipv4}]]}
```

Syntax Description	default (Optional) Displays information about the default permission list.
details	(Optional) Displays attached access control list (ACL) details.
ipv4	(Optional) Displays information about the IPv4 protocol.
from	(Optional) Displays information about the source group.
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.

Command Modes	Privileged EXE (#)			
Command History	Release	Modification		
	Cisco IOS XE Denali 16.3.1 This command was introduced.			
Usage Guidelines				
<p>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.</p> <p>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).</p> <p>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.</p>				
<p>The following is sample output from the show role-based permissions command:</p> <pre>Switch# show cts role-based permissions IPv4 Role-based permissions default (monitored): default_sgacl-02 Permit IP-00 IPv4 Role-based permissions from group 305:sgt to group 306:dgt (monitored): test_reg_tcp_permit-02 RBACL Monitor All for Dynamic Policies : TRUE RBACL Monitor All for Configured Policies : FALSE IPv4 Role-based permissions from group 6:SGT_6 to group 6:SGT_6 (configured): mon_1 IPv4 Role-based permissions from group 10 to group 11 (configured): mon_2 RBACL Monitor All for Dynamic Policies : FALSE RBACL Monitor All for Configured Policies : FALSE</pre>				

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

show cisp

To display CISP information for a specified interface, use the **show cisp** command in privileged EXEC mode.

show cisp { [clients | interface *interface-id*] | registrations | summary}

Syntax Description	clients	(Optional) Display CISP client details.
---------------------------	----------------	---

show cisp

interface *interface-id* (Optional) Display CISP information about the specified interface. Valid interfaces include physical ports and port channels.

registrations Displays CISP registrations.

summary (Optional) Displays CISP summary.

Command Modes Privileged EXEC

Command History	Release	Modification
------------------------	----------------	---------------------

Cisco IOS XE Everest 16.6.1	This command was introduced.
-----------------------------	------------------------------

	This command was reintroduced. This command was not supported in and
--	--

This example shows output from the **show cisp interface** command:

```
Device# show cisp interface fast 0
CISP not enabled on specified interface
```

This example shows output from the **show cisp registration** command:

```
Device# show cisp registrations
Interface(s) with CISP registered user(s):
-----
Fa1/0/13
Auth Mgr (Authenticator)
Gi2/0/1
Auth Mgr (Authenticator)
Gi2/0/2
Auth Mgr (Authenticator)
Gi2/0/3
Auth Mgr (Authenticator)
Gi2/0/5
Auth Mgr (Authenticator)
Gi2/0/9
Auth Mgr (Authenticator)
Gi2/0/11
Auth Mgr (Authenticator)
Gi2/0/13
Auth Mgr (Authenticator)
Gi3/0/3
Gi3/0/5
Gi3/0/23
```

Related Commands

Command	Description
cisp enable	Enable Client Information Signalling Protocol (CISP)
dot1x credentials <i>profile</i>	Configure a profile on a supplicant switch

show dot1x

To display IEEE 802.1x statistics, administrative status, and operational status for the switch or for the specified port, use the **show dot1x** command in user EXEC mode.

```
show dot1x [all [count | details | statistics | summary]] [interface type number [details | statistics] ] [statistics]
```

Syntax Description		
all	(Optional) Displays the IEEE 802.1x information for all interfaces.	
count	(Optional) Displays total number of authorized and unauthorized clients.	
details	(Optional) Displays the IEEE 802.1x interface details.	
statistics	(Optional) Displays the IEEE 802.1x statistics for all interfaces.	
summary	(Optional) Displays the IEEE 802.1x summary for all interfaces.	
interface type number	(Optional) Displays the IEEE 802.1x status for the specified port.	
Command Modes	User EXEC	
Command History	Release	Modification
Cisco IOS XE Everest 16.6.1		This command was introduced.

This is an example of output from the **show dot1x all** command:

```
Device# show dot1x all
Sysauthcontrol           Enabled
Dot1x Protocol Version   3
```

This is an example of output from the **show dot1x all count** command:

```
Device# show dot1x all count
Number of Dot1x sessions
-----
Authorized Clients      = 0
UnAuthorized Clients    = 0
Total No of Client      = 0
```

This is an example of output from the **show dot1x all statistics** command:

```
Device# show dot1x statistics
Dot1x Global Statistics for
-----
RxStart = 0      RxLogoff = 0      RxResp = 0      RxRespID = 0
RxReq = 0       RxInvalid = 0     RxLenErr = 0
RxTotal = 0
```

show eap pac peer

```

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 Everest 16.6.1	This command was introduced.

This is an example of output from the **show eap pac peers** privileged EXEC command:

```
Device> show eap pac peers
No PACs stored
```

Related Commands	Command	Description
	clear eap sessions	Clears EAP session information for the switch or for the specified port.

show ip dhcp snooping statistics

To display DHCP snooping statistics in summary or detail form, use the **show ip dhcp snooping statistics** command in user EXEC mode.

show ip dhcp snooping statistics [detail]

Syntax Description	detail (Optional) Displays detailed statistics information.
---------------------------	--

Command Modes	User EXEC
----------------------	-----------

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines In a switch stack, all statistics are generated on the stack master. If a new active switch is elected, the statistics counters reset.

This is an example of output from the **show ip dhcp snooping statistics** command:

```
Device> show ip dhcp snooping statistics
```

Packets Forwarded	= 0
Packets Dropped	= 0
Packets Dropped From untrusted ports	= 0

This is an example of output from the **show ip dhcp snooping statistics detail** command:

```
Device> show ip dhcp snooping statistics detail
```

Packets Processed by DHCP Snooping	= 0
Packets Dropped Because	
IDB not known	= 0
Queue full	= 0
Interface is in errdisabled	= 0
Rate limit exceeded	= 0
Received on untrusted ports	= 0
Nonzero giaddr	= 0
Source mac not equal to chaddr	= 0
Binding mismatch	= 0
Insertion of opt82 fail	= 0
Interface Down	= 0
Unknown output interface	= 0
Reply output port equal to input port	= 0
Packet denied by platform	= 0

This table shows the DHCP snooping statistics and their descriptions:

Table 168: 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.

```
show ip dhcp snooping statistics
```

DHCP Snooping Statistic	Description
Interface is in errdisabled	Number of times a packet was received on a port that has been marked as error disabled. This might happen if packets are in the processing queue when a port is put into the error-disabled state and those packets are subsequently processed.
Rate limit exceeded	Number of times the rate limit configured on the port was exceeded and the interface was put into the error-disabled state.
Received on untrusted ports	Number of times a DHCP server packet (OFFER, ACK, NAK, or LEASEQUERY) was received on an untrusted port and was dropped.
Nonzero giaddr	Number of times the relay agent address field (giaddr) in the DHCP packet received on an untrusted port was not zero, or the no ip dhcp snooping information option allow-untrusted global configuration command is not configured and a packet received on an untrusted port contained option-82 data.
Source mac not equal to chaddr	Number of times the client MAC address field of the DHCP packet (chaddr) does not match the packet source MAC address and the ip dhcp snooping verify mac-address global configuration command is configured.
Binding mismatch	Number of times a RELEASE or DECLINE packet was received on a port that is different than the port in the binding for that MAC address-VLAN pair. This indicates someone might be trying to spoof the real client, or it could mean that the client has moved to another port on the switch and issued a RELEASE or DECLINE. The MAC address is taken from the chaddr field of the DHCP packet, not the source MAC address in the Ethernet header.
Insertion of opt82 fail	Number of times the option-82 insertion into a packet failed. The insertion might fail if the packet with the option-82 data exceeds the size of a single physical packet on the internet.
Interface Down	Number of times the packet is a reply to the DHCP relay agent, but the SVI interface for the relay agent is down. This is an unlikely error that occurs if the SVI goes down between sending the client request to the DHCP server and receiving the response.
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.

DHCP Snooping Statistic	Description
Packet denied by platform	Number of times the packet has been denied by a platform-specific registry.

show radius server-group

To display properties for the RADIUS server group, use the **show radius server-group** command.

show radius server-group {name | all}

Syntax Description

name	Name of the server group. The character string used to name the group of servers must be defined using the aaa group server radius command.
all	Displays properties for all of the server groups.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines

Use the **show radius server-group** command to display the server groups that you defined by using the **aaa group server radius** command.

This is an example of output from the **show radius server-group all** command:

```
Device# show radius server-group all
Server group radius
  Sharecount = 1  sg_unconfigured = FALSE
  Type = standard  Memlocks = 1
```

This table describes the significant fields shown in the display.

Table 169: 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.

show vlan access-map

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 vlan access-map

To display information about a particular VLAN access map or for all VLAN access maps, use the **show vlan access-map** command in privileged EXEC mode.

show vlan access-map [map-name]

Syntax Description	<i>map-name</i> (Optional) Name of a specific VLAN access map.				
Command Default	None				
Command Modes	Privileged EXEC				
Command History	<table> <tr> <td>Release</td> <td>Modification</td> </tr> <tr> <td>Cisco IOS XE Everest 16.6.1</td> <td>This command was introduced.</td> </tr> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				

This is an example of output from the **show vlan access-map** command:

```
Device# show vlan access-map
Vlan access-map "vmap4" 10
  Match clauses:
    ip address: a12
  Action:
    forward
Vlan access-map "vmap4" 20
  Match clauses:
    ip address: a12
  Action:
    forward
```

show vlan filter

To display information about all VLAN filters or about a particular VLAN or VLAN access map, use the **show vlan filter** command in privileged EXEC mode.

```
show vlan filter {access-map name | vlan vlan-id}
```

Syntax Description	access-map <i>name</i> (Optional) Displays filtering information for the specified VLAN access map.				
	vlan <i>vlan-id</i> (Optional) Displays filtering information for the specified VLAN. The range is 1 to 4094.				
Command Default	None				
Command Modes	Privileged EXEC				
Command History	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; padding-bottom: 2px;">Release</th><th style="text-align: right; padding-bottom: 2px;">Modification</th></tr> </thead> <tbody> <tr> <td style="padding-top: 2px;">Cisco IOS XE Everest 16.6.1</td><td style="text-align: right; padding-top: 2px;">This command was introduced.</td></tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				

This is an example of output from the **show vlan filter** command:

```
Device# show vlan filter
VLAN Map map_1 is filtering VLANs:
 20-22
```

show vlan group

To display the VLANs that are mapped to VLAN groups, use the **show vlan group** command in privileged EXEC mode.

```
show vlan group [{group-name vlan-group-name [user_count]}]
```

Syntax Description	group-name <i>vlan-group-name</i> (Optional) Displays the VLANs mapped to the specified VLAN group.				
	user_count (Optional) Displays the number of users in each VLAN mapped to a specified VLAN group.				
Command Default	None				
Command Modes	Privileged EXEC				
Command History	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; padding-bottom: 2px;">Release</th><th style="text-align: right; padding-bottom: 2px;">Modification</th></tr> </thead> <tbody> <tr> <td style="padding-top: 2px;">Cisco IOS XE Everest 16.6.1</td><td style="text-align: right; padding-top: 2px;">This command was introduced.</td></tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				

switchport port-security aging**Usage Guidelines**

The **show vlan group** command displays the existing VLAN groups and lists the VLANs and VLAN ranges that are members of each VLAN group. If you enter the **group-name** keyword, only the members of the specified VLAN group are displayed.

This example shows how to display the members of a specified VLAN group:

switchport port-security aging

To set the aging time and type for secure address entries or to change the aging behavior for secure addresses on a particular port, use the **switchport port-security aging** command in interface configuration mode. To disable port security aging or to set the parameters to their default states, use the **no** form of this command.

```
switchport port-security aging {static | time time | type {absolute | inactivity}}
no switchport port-security aging {static | time | type}
```

Syntax Description

static	Enables aging for statically configured secure addresses on this port.
time <i>time</i>	Specifies the aging time for this port. The range is 0 to 1440 minutes. If the time is 0, aging is disabled for this port.
type	Sets the aging type.
absolute	Sets absolute aging type. All the secure addresses on this port age out exactly after the time (minutes) specified and are removed from the secure address list.
inactivity	Sets the inactivity aging type. The secure addresses on this port age out only if there is no data traffic from the secure source address for the specified time period.

Command Default

The port security aging feature is disabled. The default time is 0 minutes.

The default aging type is absolute.

The default static aging behavior is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE Everest 16.6.1	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 becomes inactive, and other addresses can become secure.

To allow unlimited access to a secure address, configure it as a secure address, and disable aging for the statically configured secure address by using the **no switchport port-security aging static** interface configuration command.

This example sets the aging time as 2 hours for absolute aging for all the secure addresses on the port:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# switchport port-security aging time 120
```

This example sets the aging time as 2 minutes for inactivity aging type with aging enabled for configured secure addresses on the port:

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# switchport port-security aging time 2
Device(config-if)# switchport port-security aging type inactivity
Device(config-if)# switchport port-security aging static
```

This example shows how to disable aging for configured secure addresses:

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# no switchport port-security aging static
```

switchport port-security mac-address

To configure secure MAC addresses or sticky MAC address learning, use the **switchport port-security mac-address** interface configuration command. To return to the default setting, use the **no** form of this command.

```
switchport port-security mac-address {mac-address [{vlan {vlan-id {access | voice}}}] | sticky [{mac-address | vlan {vlan-id {access | voice}}}]}
no switchport port-security mac-address {mac-address [{vlan {vlan-id {access | voice}}}] | sticky [{mac-address | vlan {vlan-id {access | voice}}}]}
```

Syntax Description

mac-address A secure MAC address for the interface by entering a 48-bit MAC address. You can add additional secure MAC addresses up to the maximum value configured.

vlan vlan-id (Optional) On a trunk port only, specifies the VLAN ID and the MAC address. If no VLAN ID is specified, the native VLAN is used.

vlan access (Optional) On an access port only, specifies the VLAN as an access VLAN.

vlan voice (Optional) On an access port only, specifies the VLAN as a voice VLAN.

Note The **voice** keyword is available only if voice VLAN is configured on a port and if that port is not the access VLAN.

sticky Enables the interface for sticky learning. When sticky learning is enabled, the interface adds all secure MAC addresses that are dynamically learned to the running configuration and converts these addresses to sticky secure MAC addresses.

mac-address (Optional) A MAC address to specify a sticky secure MAC address.

Command Default

No secure MAC addresses are configured.

Sticky learning is disabled.

switchport port-security mac-address

Command Modes	Interface configuration	
Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines	A secure port has the following limitations: <ul style="list-style-type: none"> • A secure port can be an access port or a trunk port; it cannot be a dynamic access port. • A secure port cannot be a routed port. • A secure port cannot be a protected port. • A secure port cannot be a destination port for Switched Port Analyzer (SPAN). • A secure port cannot belong to a Gigabit or 10-Gigabit EtherChannel port group. • You cannot configure static secure or sticky secure MAC addresses in the voice VLAN. • When you enable port security on an interface that is also configured with a voice VLAN, set the maximum allowed secure addresses on the port to two. When the port is connected to a Cisco IP phone, the IP phone requires one MAC address. The Cisco IP phone address is learned on the voice VLAN, but is not learned on the access VLAN. If you connect a single PC to the Cisco IP phone, no additional MAC addresses are required. If you connect more than one PC to the Cisco IP phone, you must configure enough secure addresses to allow one for each PC and one for the Cisco IP phone. • Voice VLAN is supported only on access ports and not on trunk ports.
-------------------------	---

Sticky secure MAC addresses have these characteristics:

- When you enable sticky learning on an interface by using the **switchport port-security mac-address sticky** interface configuration command, the interface converts all the dynamic secure MAC addresses, including those that were dynamically learned before sticky learning was enabled, to sticky secure MAC addresses and adds all sticky secure MAC addresses to the running configuration.
- If you disable sticky learning by using the **no switchport port-security mac-address sticky** interface configuration command or the running configuration is removed, the sticky secure MAC addresses remain part of the running configuration but are removed from the address table. The addresses that were removed can be dynamically reconfigured and added to the address table as dynamic addresses.
- When you configure sticky secure MAC addresses by using the **switchport port-security mac-address sticky mac-address** interface configuration command, these addresses are added to the address table and the running configuration. If port security is disabled, the sticky secure MAC addresses remain in the running configuration.
- If you save the sticky secure MAC addresses in the configuration file, when the switch restarts or the interface shuts down, the interface does not need to relearn these addresses. If you do not save the sticky secure addresses, they are lost. If sticky learning is disabled, the sticky secure MAC addresses are converted to dynamic secure addresses and are removed from the running configuration.
- If you disable sticky learning and enter the **switchport port-security mac-address sticky mac-address** interface configuration command, an error message appears, and the sticky secure MAC address is not added to the running configuration.

You can verify your settings by using the **show port-security** privileged EXEC command.

This example shows how to configure a secure MAC address and a VLAN ID on a port:

```
Device(config)# interface gigabitethernet 2/0/2
Device(config-if)# switchport mode trunk
Device(config-if)# switchport port-security
Device(config-if)# switchport port-security mac-address 1000.2000.3000 vlan 3
```

This example shows how to enable sticky learning and to enter two sticky secure MAC addresses on a port:

```
Device(config)# interface gigabitethernet 2/0/2
Device(config-if)# switchport port-security mac-address sticky
Device(config-if)# switchport port-security mac-address sticky 0000.0000.4141
Device(config-if)# switchport port-security mac-address sticky 0000.0000.000f
```

switchport port-security maximum

To configure the maximum number of secure MAC addresses, use the **switchport port-security maximum** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

switchport port-security maximum value [vlan [{vlan-list} [{access | voice}}]]
no switchport port-security maximum value [vlan [{vlan-list} [{access | voice}}]]

Syntax Description

value Sets the maximum number of secure MAC addresses for the interface.

The default setting is 1.

vlan (Optional) For trunk ports, sets the maximum number of secure MAC addresses on a VLAN or range of VLANs. If the **vlan** keyword is not entered, the default value is used.

vlan-list (Optional) Range of VLANs separated by a hyphen or a series of VLANs separated by commas. For nonspecified VLANs, the per-VLAN maximum value is used.

access (Optional) On an access port only, specifies the VLAN as an access VLAN.

voice (Optional) On an access port only, specifies the VLAN as a voice VLAN.

Note The **voice** keyword is available only if voice VLAN is configured on a port and if that port is not the access VLAN.

Command Default

When port security is enabled and no keywords are entered, the default maximum number of secure MAC addresses is 1.

Command Modes

Interface configuration

Command History

Release

Cisco IOS XE Everest 16.6.1

Modification

This command was introduced.

Usage Guidelines

The maximum number of secure MAC addresses that you can configure on a switch or switch stack is set by the maximum number of available MAC addresses allowed in the system. This number is determined by the

switchport port-security violation

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** privileged EXEC command.

This example shows how to enable port security on a port and to set the maximum number of secure addresses to 5. The violation mode is the default, and no secure MAC addresses are configured.

```
Device(config)# interface gigabitethernet 2/0/2
Device(config-if)# switchport mode access
Device(config-if)# switchport port-security
Device(config-if)# switchport port-security maximum 5
```

switchport port-security violation

To configure secure MAC address violation mode or the action to be taken if port security is violated, use the **switchport port-security violation** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

switchport port-security violation {protect | restrict | shutdown | shutdown vlan}
no switchport port-security violation {protect | restrict | shutdown | shutdown vlan}

Syntax Description	<p>protect Sets the security violation protect mode.</p> <p>restrict Sets the security violation restrict mode.</p> <p>shutdown Sets the security violation shutdown mode.</p> <p>shutdown Sets the security violation mode to per-VLAN shutdown. vlan</p>				
Command Default	The default violation mode is shutdown .				
Command Modes	Interface configuration				
Command History	<table border="1"> <thead> <tr> <th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td><td>This command was introduced.</td></tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				
Usage Guidelines	<p>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.</p> <p> 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.</p> <p>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.</p> <p>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.</p> <p>When the security violation mode is set to per-VLAN shutdown, only the VLAN on which the violation occurred is error-disabled.</p> <p>A secure port has the following limitations:</p> <ul style="list-style-type: none"> • 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 show how to configure a port to shut down only the VLAN if a MAC security violation occurs:

```
Device(config)# interface gigabitethernet2/0/2
Device(config)# switchport port-security violation shutdown vlan
```

tacacs server

To configure the TACACS+ server for IPv6 or IPv4 and enter TACACS+ server configuration mode, use the **tacacs server** command in global configuration mode. To remove the configuration, use the **no** form of this command.

```
tacacs server name
no tacacs server
```

Syntax Description	name Name of the private TACACS+ server host.
---------------------------	--

Command Default	No TACACS+ server is configured.
------------------------	----------------------------------

Command Modes	Global configuration (config)
----------------------	-------------------------------

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines	The tacacs server command configures the TACACS server using the <i>name</i> argument and enters TACACS+ server configuration mode. The configuration is applied once you have finished configuration and exited TACACS+ server configuration mode.
-------------------------	--

Examples	The following example shows how to configure the TACACS server using the name server1 and enter TACACS+ server configuration mode to perform further configuration:
-----------------	---

```
Device(config)# tacacs server server1
Device(config-server-tacacs) #
```

Related Commands	Command	Description
	address ipv6 (TACACS+)	Configures the IPv6 address of the TACACS+ server.
	key (TACACS+)	Configures the per-server encryption key on the TACACS+ server.
	port (TACACS+)	Specifies the TCP port to be used for TACACS+ connections.
	send-nat-address (TACACS+)	Sends a client's post-NAT address to the TACACS+ server.
	single-connection (TACACS+)	Enables all TACACS packets to be sent to the same server using a single TCP connection.
	timeout (TACACS+)	Configures the time to wait for a reply from the specified TACACS server.

tracking (IPv6 snooping)

To override the default tracking policy on a port, use the **tracking** command in IPv6 snooping policy configuration mode.

tracking {enable [reachable-lifetime {value | infinite}] | disable [stale-lifetime {value | infinite}]}

Syntax Description		
	enable	Enables tracking.
	reachable-lifetime	(Optional) Specifies the maximum amount of time a reachable entry is considered to be directly or indirectly reachable without proof of reachability. <ul style="list-style-type: none"> The reachable-lifetime keyword can be used only with the enable keyword. Use of the reachable-lifetime keyword overrides the global reachable lifetime configured by the ipv6 neighbor binding reachable-lifetime command.
	value	Lifetime value, in seconds. The range is from 1 to 86400, and the default is 300.
	infinite	Keeps an entry in a reachable or stale state for an infinite amount of time.
	disable	Disables tracking.

stale-lifetime (Optional) Keeps the time entry in a stale state, which overwrites the global stale-lifetime configuration.

- The stale lifetime is 86,400 seconds.
 - The **stale-lifetime** keyword can be used only with the **disable** keyword.
 - Use of the **stale-lifetime** keyword overrides the global stale lifetime configured by the **ipv6 neighbor binding stale-lifetime** command.
-

Command Default The time entry is kept in a reachable state.

Command Modes IPv6 snooping configuration

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines The **tracking** command overrides the default tracking policy set by the **ipv6 neighbor tracking** command on the port on which this policy applies. This function is useful on trusted ports where, for example, you may not want to track entries but want an entry to stay in the binding table to prevent it from being stolen.

The **reachable-lifetime** keyword is the maximum time an entry will be considered reachable without proof of reachability, either directly through tracking or indirectly through IPv6 snooping. After the **reachable-lifetime** value is reached, the entry is moved to stale. Use of the **reachable-lifetime** keyword with the tracking command overrides the global reachable lifetime configured by the **ipv6 neighbor binding reachable-lifetime** command.

The **stale-lifetime** keyword is the maximum time an entry is kept in the table before it is deleted or the entry is proven to be reachable, either directly or indirectly. Use of the **reachable-lifetime** keyword with the **tracking** command overrides the global stale lifetime configured by the **ipv6 neighbor binding stale-lifetime** command.

This example shows how to define an IPv6 snooping policy name as policy1, place the switch in IPv6 snooping policy configuration mode, and configure an entry to stay in the binding table for an infinite length of time on a trusted port:

```
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# tracking disable stale-lifetime infinite
```

trusted-port

To configure a port to become a trusted port, use the **trusted-port** command in IPv6 snooping policy mode or ND inspection policy configuration mode. To disable this function, use the **no** form of this command.

trusted-port
no trusted-port

Syntax Description	This command has no arguments or keywords.				
Command Default	No ports are trusted.				
Command Modes	ND inspection policy configuration IPv6 snooping configuration				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				

Usage Guidelines	When the trusted-port command is enabled, limited or no verification is performed when messages are received on ports that have this policy. However, to protect against address spoofing, messages are analyzed so that the binding information that they carry can be used to maintain the binding table. Bindings discovered from these ports will be considered more trustworthy than bindings received from ports that are not configured to be trusted.
-------------------------	--

This example shows how to define an NDP policy name as policy1, place the switch in NDP inspection policy configuration mode, and configure the port to be trusted:

```
Device(config)# ipv6 nd inspection policy1
Device(config-nd-inspection)# trusted-port
```

This example shows how to define an IPv6 snooping policy name as policy1, place the switch in IPv6 snooping policy configuration mode, and configure the port to be trusted:

```
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# trusted-port
```

vlan access-map

To create or modify a VLAN map entry for VLAN packet filtering, and change the mode to the VLAN access-map configuration, use the **vlan access-map** command in global configuration mode on the switch stack or on a standalone switch. To delete a VLAN map entry, use the **no** form of this command.

```
vlan access-map name [number]
no vlan access-map name [number]
```



Note This command is not supported on switches running the LAN Base feature set.

Syntax Description	<i>name</i> Name of the VLAN map.
---------------------------	-----------------------------------

vlan access-map

number (Optional) The sequence number of the map entry that you want to create or modify (0 to 65535). If you are creating a VLAN map and the sequence number is not specified, it is automatically assigned in increments of 10, starting from 10. This number is the sequence to insert to, or delete from, a VLAN access-map entry.

Command Default

There are no VLAN map entries and no VLAN maps applied to a VLAN.

Command Modes

Global configuration

Command History**Release****Modification**

Cisco IOS XE Everest 16.6.1

This command was introduced.

Usage Guidelines

In global configuration mode, use this command to create or modify a VLAN map. This entry changes the mode to VLAN access-map configuration, where you can use the **match** access-map configuration command to specify the access lists for IP or non-IP traffic to match and use the **action** command to set whether a match causes the packet to be forwarded or dropped.

In VLAN access-map configuration mode, these commands are available:

- **action**—Sets the action to be taken (forward or drop).
- **default**—Sets a command to its defaults.
- **exit**—Exits from VLAN access-map configuration mode.
- **match**—Sets the values to match (IP address or MAC address).
- **no**—Negates a command or set its defaults.

When you do not specify an entry number (sequence number), it is added to the end of the map.

There can be only one VLAN map per VLAN and it is applied as packets are received by a VLAN.

You can use the **no vlan access-map name [number]** command with a sequence number to delete a single entry.

Use the **vlan filter** interface configuration command to apply a VLAN map to one or more VLANs.

For more information about VLAN map entries, see the software configuration guide for this release.

This example shows how to create a VLAN map named vac1 and apply matching conditions and actions to it. If no other entries already exist in the map, this will be entry 10.

```
Device(config)# vlan access-map vac1
Device(config-access-map)# match ip address acl1
Device(config-access-map)# action forward
```

This example shows how to delete VLAN map vac1:

```
Device(config)# no vlan access-map vac1
```

vlan 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 on the switch stack or on a standalone switch. To remove the map, use the **no** form of this command.

vlan group

```
vlan filter mapname vlan-list {list | all}
no vlan filter mapname vlan-list {list | all}
```

**Note**

This command is not supported on switches running the LAN Base feature set.

Syntax Description

mapname Name of the VLAN map entry.

vlan-list Specifies which VLANs to apply the map to.

list The list of one or more VLANs in the form *tt, uu-vv, xx, yy-zz*, where spaces around commas and dashes are optional. The range is 1 to 4094.

all Adds the map to all VLANs.

Command Default

There are no VLAN filters.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines

To avoid accidentally dropping too many packets and disabling connectivity in the middle of the configuration process, we recommend that you completely define the VLAN access map before applying it to a VLAN.

For more information about VLAN map entries, see the software configuration guide for this release.

This example applies VLAN map entry *map1* to VLANs 20 and 30:

```
Device(config)# vlan filter map1 vlan-list 20, 30
```

This example shows how to delete VLAN map entry *mac1* from VLAN 20:

```
Device(config)# no vlan filter map1 vlan-list 20
```

You can verify your settings by entering the **show vlan filter** privileged EXEC command.

vlan group

To create or modify a VLAN group, use the **vlan group** command in global configuration mode. To remove a VLAN list from the VLAN group, use the **no** form of this command.

```
vlan group group-name vlan-list vlan-list
no vlan group group-name vlan-list vlan-list
```

Syntax Description

<i>group-name</i>	Name of the VLAN group. The group name may contain up to 32 characters and must begin with a letter.
-------------------	--

vlan-list *vlan-list* Specifies one or more VLANs to be added to the VLAN group. The *vlan-list* argument can be a single VLAN ID, a list of VLAN IDs, or VLAN ID range. Multiple entries are separated by a hyphen (-) or a comma (,).

Command Default None

Command Modes Global configuration

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines If the named VLAN group does not exist, the **vlan group** command creates the group and maps the specified VLAN list to the group. If the named VLAN group exists, the specified VLAN list is mapped to the group.

The **no** form of the **vlan group** command removes the specified VLAN list from the VLAN group. When you remove the last VLAN from the VLAN group, the VLAN group is deleted.

A maximum of 100 VLAN groups can be configured, and a maximum of 4094 VLANs can be mapped to a VLAN group.

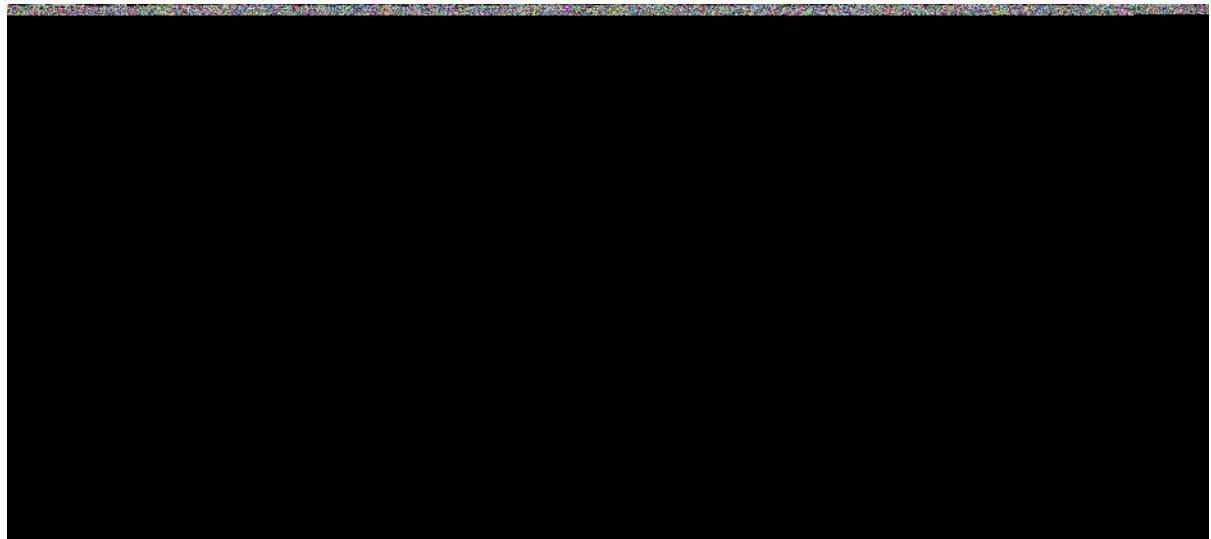
This example shows how to map VLANs 7 through 9 and 11 to a VLAN group:

```
Device(config)# vlan group group1 vlan-list 7-9,11
```

This example shows how to remove VLAN 7 from the VLAN group:

```
Device(config)# no vlan group group1 vlan-list 7
```

vlan group



PART **XIII**

System Management

- [System Management Commands, on page 1027](#)
- [Tracing, on page 1095](#)

System Management Commands

- [arp](#), on page 1028
- [boot](#), on page 1029
- [cat](#), on page 1030
- [copy](#), on page 1030
- [copy startup-config tftp:](#), on page 1031
- [copy tftp: startup-config](#), on page 1032
- [debug voice diagnostics mac-address](#), on page 1033
- [delete](#), on page 1033
- [dir](#), on page 1034
- [exit](#), on page 1035
- [flash_init](#), on page 1035
- [help](#), on page 1036
- [hw-module slot shutdown](#), on page 1037
- [hw-module subslot oir power-cycle](#), on page 1037
- [install](#), on page 1038
- [l2 traceroute](#), on page 1042
- [license boot level](#), on page 1042
- [license smart deregister](#), on page 1043
- [license smart register idtoken](#), on page 1044
- [license smart renew](#), on page 1045
- [location](#), on page 1046
- [location plm calibrating](#), on page 1049
- [mac address-table move update](#), on page 1049
- [mgmt_init](#), on page 1050
- [mkdir](#), on page 1051
- [more](#), on page 1052
- [no debug all](#), on page 1052
- [power budget mode](#), on page 1053
- [rename](#), on page 1054
- [reset](#), on page 1054
- [rmdir](#), on page 1055
- [sdm prefer](#), on page 1056
- [service private-config-encryption](#), on page 1056

- [set, on page 1057](#)
- [show cable-diagnostics tdr, on page 1059](#)
- [show debug, on page 1061](#)
- [show env, on page 1062](#)
- [show env xps, on page 1066](#)
- [show flow monitor, on page 1069](#)
- [show install, on page 1071](#)
- [show license all, on page 1073](#)
- [show license status, on page 1075](#)
- [show license summary, on page 1076](#)
- [show license udi, on page 1077](#)
- [show license usage, on page 1077](#)
- [show location, on page 1078](#)
- [show mac address-table move update, on page 1079](#)
- [show parser encrypt file status, on page 1080](#)
- [show platform integrity, on page 1081](#)
- [show platform sudi certificate, on page 1082](#)
- [show sdm prefer, on page 1083](#)
- [show tech-support license , on page 1084](#)
- [test cable-diagnostics tdr, on page 1085](#)
- [traceroute mac, on page 1086](#)
- [traceroute mac ip, on page 1089](#)
- [type, on page 1091](#)
- [unset, on page 1092](#)
- [version, on page 1093](#)

arp

To display the contents of the Address Resolution Protocol (ARP) table, use the **arp** command in boot loader mode.

arp [ip_address]

Syntax Description	<i>ip_address</i> (Optional) Shows the ARP table or the mapping for a specific IP address.				
Command Default	No default behavior or values.				
Command Modes	Boot loader				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				
Usage Guidelines	The ARP table contains the IP-address-to-MAC-address mappings.				

Examples

This example shows how to display the ARP table:

```
Device: arp 172.20.136.8
arp'ing 172.20.136.8...
172.20.136.8 is at 00:1b:78:d1:25:ae, via port 0
```

boot

To load and boot an executable image and display the command-line interface (CLI), use the **boot** command in boot loader mode.

boot [-post | -n | -p | flag] filesystem:/file-url...

Syntax Description

-post	(Optional) Run the loaded image with an extended or comprehensive power-on self-test (POST). Using this keyword causes POST to take longer to complete.
-n	(Optional) Pause for the Cisco IOS Debugger immediately after launching.
-p	(Optional) Pause for the JTAG Debugger right after loading the image.
<i>filesystem:</i>	Alias for a file system. Use flash: for the system board flash device; use usbflash0: for USB memory sticks.
<i>/file-url</i>	Path (directory) and name of a bootable image. Separate image names with a semicolon.

Command Default

No default behavior or values.

Command Modes

Boot loader

Command History**Release** **Modification**

Cisco IOS XE Everest 16.6.1 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:

cat

```
Device: set BOOT flash:/new-images/new-image.bin
Device: boot
```

After entering this command, you are prompted to start the setup program.

cat

To display the contents of one or more files, use the **cat** command in boot loader mode.

cat *filesystem:/file-url...*

Syntax Description

filesystem: Specifies a file system.

/file-url Specifies the path (directory) and name of the files to display. Separate each filename with a space.

Command Default

No default behavior or values.

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE Everest 16.6.1	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	<p><i>filesystem:</i> Alias for a file system. Use usbflash0: for USB memory sticks.</p> <p><i>/source-file-url</i> Path (directory) and filename (source) to be copied.</p> <p><i>/destination-file-url</i> Path (directory) and filename of the destination.</p>
---------------------------	---

Command Default	No default behavior or values.
------------------------	--------------------------------

Command Modes	Boot loader
----------------------	-------------

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines	<p>Filenames and directory names are case sensitive.</p> <p>Directory names are limited to 127 characters between the slashes (/); the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.</p> <p>Filenames are limited to 127 characters; the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.</p> <p>If you are copying a file to a new directory, the directory must already exist.</p>
-------------------------	---

Examples	This example shows how to copy a file at the root:
-----------------	--

```
Device: copy usbflash0:test1.text usbflash0:test4.text
File "usbflash0:test1.text" successfully copied to "usbflash0:test4.text"
```

You can verify that the file was copied by entering the **dir filesystem:** boot loader command.

copy startup-config tftp:

To copy the configuration settings from a switch to a TFTP server, use the **copy startup-config tftp:** command in Privileged EXEC mode.

copy startup-config tftp: remote host {ip-address}/{name}

Syntax Description	<i>remote host {ip-address}/{name}</i> Host name or IP-address of Remote host.
---------------------------	--

Command Default	No default behavior or values.
------------------------	--------------------------------

Command Modes	Privileged EXEC
----------------------	-----------------

copy tftp: startup-config

Command History	Release	Modification
	Cisco IOS XE Release 16.1	This command was introduced.
Usage Guidelines	To copy your current configurations from the switch, run the command copy startup-config tftp: and follow the instructions. The configurations are copied onto the TFTP server.	
	Then, login to another switch and run the command copy tftp: startup-config and follow the instructions. The configurations are now copied onto the other switch.	
Examples	This example shows how to copy the configuration settings onto a TFTP server:	

```
Device: copy startup-config tftp:  
Address or name of remote host []?
```

copy tftp: startup-config

To copy the configuration settings from a TFTP server onto a new switch, use the **copy tftp: startup-config** command in Privileged EXEC mode on the new switch.

copy tftp: startup-config *remote host {ip-address}/{name}*

Syntax Description	<i>remote host {ip-address}/{name}</i> Host name or IP-address of Remote host.	
Command Default	No default behavior or values.	
Command Modes	Privileged EXEC	
Command History	Release	Modification
	Cisco IOS XE Release 16.1	This command was introduced.
Usage Guidelines	After the configurations are copied, to save your configurations, use write memory command and then either reload the switch or run the copy startup-config running-config command.	
Examples	This example shows how to copy the configuration settings from the TFTP server onto a switch:	

```
Device: copy tftp: startup-config  
Address or name of remote host []?
```

debug voice diagnostics mac-address

To enable debugging of voice diagnostics for voice clients, use the **debug voice diagnostics mac-address** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

```
debug voice diagnostics mac-address mac-address1 verbose mac-address mac-address2 verbose
nodebug voice diagnostics mac-address mac-address1 verbose mac-address mac-address2 verbose
```

Syntax Description	voice diagnostics	Configures voice debugging for voice clients.
	mac-address 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 Everest 16.6.1	This command was introduced.	

The following is sample output from the **debug voice diagnostics mac-address** command and shows how to enable debugging of voice diagnostics for voice client with MAC address of 00:1f:ca:cf:b6:60:

```
Device# debug voice diagnostics mac-address 00:1f:ca:cf:b6:60
```

delete

To delete one or more files from the specified file system, use the **delete** command in boot loader mode.

```
delete filesystem:/file-url...
```

Syntax Description	<i>filesystem:</i> Alias for a file system. Use usbflash0: for USB memory sticks.
	<i>/file-url...</i> 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 Everest 16.6.1	This command was introduced.	

dir**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 Everest 16.6.1 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 170: dir Field Descriptions

Field	Description
2	Index number of the file.
-rwx	File permission, which can be any or all of the following: <ul style="list-style-type: none"> • d—directory • r—readable • w—writable • x—executable
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 Everest 16.6.1	This command was introduced.	

No default behavior or values.

This example shows how to exit the configuration mode:

```
Device(config)# exit
Device#
```

flash_init

To initialize the flash: file system, use the **flash_init** command in boot loader mode.

flash_init

Syntax Description This command has no arguments or keywords.

Command Default The flash: file system is automatically initialized during normal system operation.

Command Modes Boot loader

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	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 Everest 16.6.1	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
```

hw-module slot shutdown

To power down a linecard from the chassis, use the **hw-module slot shutdown** command in global configuration mode.

hw-module slot *linecard slot number* shutdown

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

Command Modes Global configuration (config)

Usage Guidelines This command is not supported on SUP slots.

A linecard need not be shut down before removing it, since surprise/live OIR is supported. This command is primarily for debugging, or when some issue is narrowed down to be caused by a particular linecard(s).

If you choose to power down a linecard by executing the **hw-module slot shutdown** command in global configuration mode and save to startup-config, the linecard will not boot no matter how many times the switch is rebooted. This command is useful when you need to shut down a linecard located in a remote location and ensure that it does not boot automatically when the switch is rebooted. To begin using the linecard again, you must manually re-enable the linecard using the **no hw-module slot shutdown** command.

```
Device(config)# hw-module slot 5 shutdown
*Nov 23 13:27:57.039 UTC: %IOSXE_OIR-6-REMSPA: SPA removed from subslot 5/0, interfaces disabled
*Nov 23 13:27:57.125 UTC: %SPA_OIR-6-OFFLINECARD: SPA (C9400-LC-48U) offline in subslot 5/0
```

hw-module subslot oir power-cycle

To reset or power-cycle a module from the CLI, use the **hw-module subslot oir power-cycle** command in privileged EXEC mode.

hw-module switch *switch-no* subslot *slot / subslot* oir power-cycle [force]

Syntax Description	<i>switch-no</i>	The switch to access. Valid values are 1 and 2.
	<i>slot</i>	Specifies the Physical slot number on the chassis.
	<i>subslot</i>	Subslot is always 0.
	force	Performs the power cycle without prompting for confirmation.

install

Command Default	No default behavior or values.				
Command Modes	Privileged EXEC				
Command History	<table border="1"> <thead> <tr> <th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.2</td><td>This command was introduced.</td></tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.2	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.2	This command was introduced.				
Usage Guidelines	<p>The hw-module subslot oir power-cycle command resets the specified module.</p> <p>This command is not supported on the supervisor slots.</p> <p>Do not use the command when the line cards are booting up.</p>				
Example	<p>The following example shows how to power-cycle the module in slot 1 of the chassis:</p> <pre>Device# hw-module switch 1 subslot 1/0 oir power-cycle force</pre> <pre>*Sep 3 20:11:05.219 UTC: %IOSXE_OIR-6-REMSPA: SPA removed from chassis 1 subslot 1/0, interfaces disabled *Sep 3 20:11:05.295 UTC: %SPA_OIR-6-OFFLINECARD: SPA (C9400-LC-24XS) offline in chassis 1 subslot 1/0 *Sep 3 20:11:36.812 UTC: %IOSXE_OIR-6-INSSPA: SPA inserted in chassis 1 subslot 1/0 *Sep 3 20:13:41.316 UTC: %SPA_OIR-6-ONLINECARD: SPA (C9400-LC-24XS) online in chassis 1 subslot 1/0</pre>				

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 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	<p>Validates whether the SMU is added through the install add command.</p> <p>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.</p>

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: rep: 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 <i>install-ID</i>	Returns to the specific install point ID. Valid values are from 1 to 4294967295.

Command Default

Packages are not installed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced.
Cisco IOS XE Fuji 16.9.1	Hot-patching support is introduced. Sample output updated with hot SMU outputs.

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 package 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 scripts done.

--- Starting SMU Activate operation ---
Performing SMU_ACTIVATE on all members
[1] SMU_ACTIVATE package(s) on switch 1
[1] Finished SMU ACTIVATE on switch 1
Checking status of SMU_ACTIVATE on [1]
SMU_ACTIVATE: Passed on [1]
Finished SMU Activate operation

SUCCESS: install_activate
/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 scripts done.
--- Starting SMU Commit operation ---
Performing SMU_COMMIT on all members
[1] SMU_COMMIT package(s) on switch 1
[1] Finished SMU_COMMIT on switch 1
Checking status of SMU_COMMIT on [1]
SMU_COMMIT: Passed on [1]
Finished SMU Commit operation

SUCCESS: install_commit
/flash/cat9k_iosxe.BLD_SMU_20180302_085005_TWIG_LATEST_20180306_013805.3.SSA.smu.bin Mon
Mar 5 21:51:01 PST 2018

```

Related Commands

Command	Description
show install	Displays information about the install packages.

I2 traceroute

To enable the Layer 2 traceroute server, use the **I2 traceroute** command in global configuration mode. Use the **no** form of this command to disable the Layer 2 traceroute server.

I2 traceroute
no I2 traceroute

Syntax Description	This command has no arguments or keywords.	
Command Modes	Global configuration (config#)	
Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	The command was introduced.

Usage Guidelines Layer 2 traceroute is enabled by default and opens a listening socket on User Datagram Protocol (UDP) port 2228. To close the UDP port 2228 and disable Layer 2 traceroute, use the **no I2 traceroute** command in global configuration mode.

The following example shows how to configure Layer 2 traceroute using the **I2 traceroute** command.

```
Device# configure terminal
Device(config)# I2 traceroute
```

license 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	<i>base-license-level</i> Level at which the switch is booted, for example, network-essentials
	Base licenses that are available are: <ul style="list-style-type: none">• 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-essentials* license on a switch at the next reload:

```
Device(config)# license boot level network-essentials
```

license smart deregister

To cancel device registration from Cisco Smart Software Manager (CSSM), use the **license smart deregister** command in privileged EXEC mode.

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.

license smart register idtoken

Usage GuidelinesUse 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

<i>token_ID</i>	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
$T14UytrNxBzbEs1ck8veUtWaG5abnZJOFdDa1FwbVRa%0Ab1RMbz0%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 {hostid} | civic-location identifier {hostid} |
elin-location {string | identifier id} | geo-location identifier {hostid} | prefer{cdp weight
priority-value | lldp-med weight priority-value | static config weight priority-value}
no location {admin-tag string | civic-location identifier {hostid} | civic-location identifier {hostid} |
elin-location {string | identifier id} | geo-location identifier {hostid} | prefer{cdp weight
priority-value | lldp-med weight priority-value | static config weight priority-value}
```

Syntax Description	admin-tag <i>string</i> Configures administrative tag or site information. Site or location information in alphanumeric format. civic-location Configures civic location information. identifier Specifies the name of the civic location, emergency, or geographical location. host Defines the host civic or geo-spatial location. <i>id</i> Name of the civic, emergency, or geographical location. Note The identifier for the civic location in the LLDP-MED switch TLV is limited to 250 bytes or less. To avoid error messages about available buffer space during switch configuration, be sure that the total length of all civic-location information specified for each civic-location identifier does not exceed 250 bytes.
Command Default	No default behavior or values.
Command Modes	Global configuration

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	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:	
	<ul style="list-style-type: none"> • 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	<table border="1"> <thead> <tr> <th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td><td>This command was introduced.</td></tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				

Usage Guidelines The uniband is useful for single radio clients (even if the radio is a dual band and can operate in the 2.4-GHz and the 5-GHz bands). The multiband is useful for multiple radio clients.

This example shows how to configure the path loss measurement request for calibrating clients on the associated 802.11a/b/g radio:

```
Device# configure terminal
Device(config)# location plm calibrating uniband
Device(config)# end
```

mac address-table move update

To enable the MAC address table move update feature, use the **mac address-table move update** command in global configuration mode on the switch stack or on a standalone switch. To return to the default setting, use the **no** form of this command.

mac address-table move update {receive | transmit}
no mac address-table move update {receive | transmit}

Syntax Description	receive Specifies that the switch processes MAC address-table move update messages. transmit Specifies that the switch sends MAC address-table move update messages to other switches in the network if the primary link goes down and the standby link comes up.
---------------------------	--

mgmt_init

Command Default	By default, the MAC address-table move update feature is disabled.				
Command Modes	Global configuration				
Command History					
Command History					
<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>		Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				
Usage Guidelines					
<p>The MAC address-table move update feature allows the switch to provide rapid bidirectional convergence if a primary (forwarding) link goes down and the standby link begins forwarding traffic.</p> <p>You can configure the access switch to send the MAC address-table move update messages if the primary link goes down and the standby link comes up. You can configure the uplink switches to receive and process the MAC address-table move update messages.</p>					
<h3>Examples</h3> <p>This example shows how to configure an access switch to send MAC address-table move update messages:</p> <pre>Device# configure terminal Device(config)# mac address-table move update transmit Device(config)# end</pre> <p>This example shows how to configure an uplink switch to get and process MAC address-table move update messages:</p> <pre>Device# configure terminal Device(config)# mac address-table move update receive Device(config)# end</pre>					

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 Everest 16.6.1	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 Everest 16.6.1	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

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 Everest 16.6.1	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.
```

power budget mode

To configure the system to reserve power for a single supervisor, use the **power budget mode** command in global configuration mode

```
power budget mode
single-sup
no power budget mode
single-sup
```

Command Default	The system reserves power for both supervisor modules.
-----------------	--

Command Modes	Global configuration mode (config)
---------------	------------------------------------

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

Usage Guidelines	Before you configure the command to reserve power for a single supervisor, ensure that these prerequisites are met:
------------------	---

- You have installed only one supervisor module in the chassis
- You have installed a blank in the second supervisor slot

Further guidelines related to power budgeting are available in the [software configuration guide](#). In applicable version of the guide, go to **Contents** → **System Management** → **Environmental Monitoring and Power Management** → **Power Budgeting for Supervisor Modules**.

Examples

The following example shows how you can reserve power for a single supervisor module:

```
Device# configure terminal
Device(config)# power budget mode single-sup
Device(config)# end
```

rename

rename

To rename a file, use the **rename** command in boot loader mode.

rename *filesystem:/source-file-url filesystem:/destination-file-url*

Syntax Description	<p><i>filesystem:</i> Alias for a file system. Use usbflash0: for USB memory sticks.</p> <p><i>/source-file-url</i> Original path (directory) and filename.</p> <p><i>/destination-file-url</i> New path (directory) and filename.</p>				
Command Default	No default behavior or values.				
Command Modes	Boot loader				
Command History	<table border="1"> <thead> <tr> <th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td><td>This command was introduced.</td></tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				
Usage Guidelines	<p>Filenames and directory names are case sensitive.</p> <p>Directory names are limited to 127 characters between the slashes (/); the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.</p> <p>Filenames are limited to 127 characters; the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.</p>				

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.

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 Everest 16.6.1	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	<i>filesystem:</i> Alias for a file system. Use usbflash0: for USB memory sticks.
	<i>/directory-url...</i> 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 Everest 16.6.1	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

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	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>		Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification					
Cisco IOS XE Everest 16.6.1	This command was introduced.					
Usage Guidelines	<p>In a device stack, all stack members must use the same SDM template that is stored on the active device. When a new device is added to a stack, the SDM configuration that is stored on the active device overrides the template configured on an individual device.</p>					

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 16.8.1a	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	<i>variable value</i>	Use one of the following keywords for <i>variable</i> and the appropriate value for <i>value</i> :
	MANUAL_BOOT	—Decides whether the device automatically or manually boots.
		Valid values are 1/Yes and 0/No. If it is set to 0 or No, the boot loader attempts to automatically boot the system. If it is set to anything else, you must manually boot the device from the boot loader mode.
	BOOT <i>filesystem:/file-url</i>	—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 <i>filesystem:/file-url</i>	—Identifies a semicolon-separated list of loadable files to dynamically load during the boot loader initialization. Helper files extend or patch the functionality of the boot loader.
	PS1 <i>prompt</i>	—Specifies a string that is used as the command-line prompt in boot loader mode.

set

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 Everest 16.6.1 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 cable-diagnostics tdr

To display the Time Domain Reflector (TDR) results, use the **show cable-diagnostics tdr** command in privileged EXEC mode.

show cable-diagnostics tdr interface *interface-id*

Syntax Description	<i>interface-id</i> Specifies the interface on which TDR is run.	
Command Default	No default behavior or values.	
Command Modes	Privileged EXEC	
Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.
Usage Guidelines	TDR is supported only on 10/100/100 copper Ethernet ports. It is not supported on 10-Gigabit Ethernet ports and small form-factor pluggable (SFP) module ports.	

show cable-diagnostics tdr

Examples

This example shows the output from the **show cable-diagnostics tdr interface *interface-id*** command on a device:

```
Device# show cable-diagnostics tdr interface gigabitethernet1/0/23
TDR test last run on: March 01 00:04:08
Interface  Speed  Local pair  Pair length          Remote pair  Pair status
-----  -----
Gi1/0/23   1000M  Pair A      1  +/- 1 meters    Pair A       Normal
           Pair B      1  +/- 1 meters    Pair B       Normal
           Pair C      1  +/- 1 meters    Pair C       Normal
           Pair D      1  +/- 1 meters    Pair D       Normal
```

Table 171: Field Descriptions for the show cable-diagnostics tdr Command Output

Field	Description
Interface	The interface on which TDR is run.
Speed	The speed of connection.
Local pair	The name of the pair of wires that TDR is testing on the local interface.
Pair length	The location of the problem on the cable, with respect to your device. TDR can only find the location in one of these cases: <ul style="list-style-type: none"> The cable is properly connected, the link is up, and the interface speed is 1000 Mb/s. The cable is open. The cable has a short.
Remote pair	The name of the pair of wires to which the local pair is connected. TDR can learn about the remote pair only when the cable is properly connected and the link is up.
Pair status	The status of the pair of wires on which TDR is running: <ul style="list-style-type: none"> Normal—The pair of wires is properly connected. Not completed—The test is running and is not completed. Not supported—The interface does not support TDR. Open—The pair of wires is open. Shorted—The pair of wires is shorted. ImpedanceMis—The impedance is mismatched. Short/Impedance Mismatched—The impedance mismatched or the cable is short. InProgress—The diagnostic test is in progress.

This example shows the output from the **show interface *interface-id*** command when TDR is running:

```
Device# show interface gigabitethernet1/0/2
gigabitethernet1/0/2 is up, line protocol is up (connected: TDR in Progress)
```

This example shows the output from the **show cable-diagnostics tdr interface *interface-id*** command when TDR is not running:

```
Device# show cable-diagnostics tdr interface gigabitethernet1/0/2
% TDR test was never issued on gigabitethernet1/0/2
```

If an interface does not support TDR, this message appears:

```
% TDR test is not supported on device 1
```

show debug

To display all the debug commands available on a switch, use the **show debug** command in Privileged EXEC mode.

show debug

show debug condition *Condition identifier / All conditions*

Syntax Description	<i>Condition identifier</i> Sets the value of the condition identifier to be used. Range is between 1 and 1000. <i>All conditions</i> Shows all conditional debugging options available.				
Command Default	No default behavior or values.				
Command Modes	Privileged EXEC				
Command History	<table border="1"> <thead> <tr> <th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td>Cisco IOS XE Release 16.1</td><td>This command was introduced.</td></tr> </tbody> </table>	Release	Modification	Cisco IOS XE Release 16.1	This command was introduced.
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

show env

To display the list of sensors and all details like location, operational counters, status, history and so on, for the sensors, use the **show env** command in EXEC modes.

```
show env {all | counters | history sensor-name | location sensor-name | sensor sensor-name | status | summary | table sensor-name}
```

Syntax Description

all	Displays a list of sensors on the switch.
counters	Displays the operational counters.
history sensor-name	Displays the sensor state change history.
location	Displays sensors by location.
sensor sensor-name	Displays sensor summary.
status	Displays the environmental status of the power fan units (PFU).
summary	Displays a summary of all environmental monitoring sensors.
table sensor-name	Displays sensor state table.

Command Default

No default behavior or values.

Command Modes

User EXEC

Privileged EXEC

Command History

Release

Modification

Cisco IOS XE Everest 16.6.1 This command was introduced.

Usage Guidelines

Use the **show env** privileged EXEC command to display the device sensor information.

The following example shows how to display information for a sensor:

```
Switch#show env sensor Temp
Sensor Summary: Environmental Monitoring
Sensor: Temp: Coretemp      Location: R0
Current State: Normal          Reading: 46 Celsius

Sensor: Temp: DopplerD       Location: R0
Current State: Normal          Reading: 86 Celsius

Sensor: Temp: outlet        Location: R0
Current State: Normal          Reading: 43 Celsius

Sensor: Temp: inlet         Location: R0
Current State: Normal          Reading: 43 Celsius
```

```

Sensor: Temp:   Outlet    Location: 6/0
        Current State: Normal           Reading: 39 Celsius

Sensor: Temp:   Inlet     Location: 6/0
        Current State: Normal           Reading: 36 Celsius

Sensor: Temp:   Outlet    Location: 5/0
        Current State: Normal           Reading: 33 Celsius

Sensor: Temp:   Inlet     Location: 5/0
        Current State: Normal           Reading: 28 Celsius

```

The following example shows how to display the status of different sensors:

```

Switch#show env status
Power
Supply Model No          Type Capacity Status      Fan States
----- -----
PS2    WS-XP3200AC       AC   3200 W  active   good  good  good  good
PS3    WS-XP3200AC       AC   3200 W  active   good  good  good  good

PS Current Configuration Mode : Combined
PS Current Operating State   : Combined

Power supplies currently active   : 2
Power supplies currently available : 2

Fantray : good
Power consumed by Fantray : 350 Watts
Fantray airflow direction : side-to-side
Fantray beacon LED: off
Fantray status LED: green
SYSTEM : GREEN

```

The following example shows how to display the sensor state table:

```

Switch#show env table Temp
Sensor State Table: Environmental Monitoring
Sensor: Temp: Coretemp    Location: R0
Current State: Normal           Reading: 46 Celsius
0-Normal           Low:-2147483647 High:106      Margin:0
                  Action:RECORD      Alarm:NONE
                  Poll:60000          Reminder:3600000
1-Minor            Low:107       High:116      Margin:0
                  Action:RECORD      Alarm:MINOR
                  Poll:60000          Reminder:3600000
2-Major             Low:117       High:122      Margin:0
                  Action:RECORD      Alarm:MAJOR
                  Poll:60000          Reminder:3600000
3-Critical          Low:123       High:124      Margin:0
                  Action:RECORD      Alarm:CRITICAL
                  Poll:60000          Reminder:3600000
4-Shutdown          Low:125       High:2147483647 Margin:0
                  Action:SHUTDOWN    Alarm:NONE
                  Poll:60000          Reminder:3600000

Sensor State Table: Environmental Monitoring
Sensor: Temp: DopplerD    Location: R0
Current State: Normal           Reading: 86 Celsius
0-Normal           Low:-2147483647 High:106      Margin:0
                  Action:RECORD      Alarm:NONE
                  Poll:60000          Reminder:3600000
1-Minor            Low:107       High:116      Margin:0

```

show env

```

Action:RECORD           Alarm:MINOR
Poll:60000              Reminder:3600000
2-Major                 Low:117      High:122      Margin:0
Action:RECORD           Alarm:MAJOR
Poll:60000              Reminder:3600000
3-Critical              Low:123      High:124      Margin:0
Action:RECORD           Alarm:CRITICAL
Poll:60000              Reminder:3600000
4-Shutdown               Low:125      High:2147483647 Margin:0
Action:RECORD           Alarm:CRITICAL
Poll:60000              Reminder:3600000

Sensor State Table: Environmental Monitoring
Sensor: Temp: outlet   Location: R0
Current State: Normal          Reading: 43 Celsius
0-Normal                Low:-2147483648 High:54      Margin:0
Action:RECORD           Alarm:NONE
Poll:60000              Reminder:3600000
1-Minor                 Low:55       High:64       Margin:0
Action:RECORD           Alarm:MINOR
Poll:60000              Reminder:3600000
2-Major                 Low:65       High:74       Margin:0
Action:RECORD           Alarm:MAJOR
Poll:60000              Reminder:3600000
3-Critical              Low:75       High:99       Margin:0
Action:RECORD           Alarm:CRITICAL
Poll:60000              Reminder:3600000
4-Shutdown               Low:100      High:2147483647 Margin:0
Action:SHUTDOWN          Alarm:CRITICAL
Poll:60000              Reminder:3600000

Sensor State Table: Environmental Monitoring
Sensor: Temp: inlet     Location: R0
Current State: Normal          Reading: 43 Celsius
0-Normal                Low:-2147483648 High:44      Margin:0
Action:RECORD           Alarm:NONE
Poll:60000              Reminder:3600000
1-Minor                 Low:45       High:54       Margin:0
Action:RECORD           Alarm:MINOR
Poll:60000              Reminder:3600000
2-Major                 Low:55       High:64       Margin:0
Action:RECORD           Alarm:MAJOR
Poll:60000              Reminder:3600000
3-Critical              Low:65       High:71       Margin:0
Action:RECORD           Alarm:CRITICAL
Poll:60000              Reminder:3600000
4-Shutdown               Low:72       High:2147483647 Margin:0
Action:SHUTDOWN          Alarm:CRITICAL
Poll:60000              Reminder:3600000

Sensor State Table: Environmental Monitoring
Sensor: Temp: Outlet    Location: 6/0
Current State: Normal          Reading: 39 Celsius
0-Normal                Low:-2147483648 High:54      Margin:0
Action:RECORD           Alarm:NONE
Poll:60000              Reminder:3600000
1-Minor                 Low:55       High:64       Margin:0
Action:RECORD           Alarm:MINOR
Poll:60000              Reminder:3600000
2-Major                 Low:65       High:74       Margin:0
Action:RECORD           Alarm:MAJOR
Poll:60000              Reminder:3600000
3-Critical              Low:75       High:99       Margin:0
Action:RECORD           Alarm:CRITICAL

```

```

Poll:60000           Reminder:3600000
4-Shutdown          Low:100            High:2147483647 Margin:0
Action:SHUTDOWN
Poll:60000           Reminder:3600000

Sensor State Table: Environmental Monitoring
Sensor: Temp: Inlet Location: 6/0
Current State: Normal Reading: 36 Celsius
0-Normal           Low:-2147483648 High:44 Margin:0
Action:RECORD
Poll:60000           Reminder:3600000
1-Minor             Low:45            High:54 Margin:0
Action:RECORD
Poll:60000           Reminder:3600000
2-Major              Low:55            High:64 Margin:0
Action:RECORD
Poll:60000           Reminder:3600000
3-Critical           Low:65            High:71 Margin:0
Action:RECORD
Poll:60000           Reminder:3600000
4-Shutdown           Low:72            High:2147483647 Margin:0
Action:SHUTDOWN
Poll:60000           Reminder:3600000

Sensor State Table: Environmental Monitoring
Sensor: Temp: Outlet Location: 5/0
Current State: Normal Reading: 33 Celsius
0-Normal           Low:-2147483648 High:54 Margin:0
Action:RECORD
Poll:60000           Reminder:3600000
1-Minor             Low:55            High:64 Margin:0
Action:RECORD
Poll:60000           Reminder:3600000
2-Major              Low:65            High:74 Margin:0
Action:RECORD
Poll:60000           Reminder:3600000
3-Critical           Low:75            High:99 Margin:0
Action:RECORD
Poll:60000           Reminder:3600000
4-Shutdown           Low:100           High:2147483647 Margin:0
Action:SHUTDOWN
Poll:60000           Reminder:3600000

Sensor State Table: Environmental Monitoring
Sensor: Temp: Inlet Location: 5/0
Current State: Normal Reading: 28 Celsius
0-Normal           Low:-2147483648 High:44 Margin:0
Action:RECORD
Poll:60000           Reminder:3600000
1-Minor             Low:45            High:54 Margin:0
Action:RECORD
Poll:60000           Reminder:3600000
2-Major              Low:55            High:64 Margin:0
Action:RECORD
Poll:60000           Reminder:3600000
3-Critical           Low:65            High:71 Margin:0
Action:RECORD
Poll:60000           Reminder:3600000
4-Shutdown           Low:72            High:2147483647 Margin:0
Action:SHUTDOWN
Poll:60000           Reminder:3600000

```

show env xps

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 configuration port [all number] power system thermal upgrade version	Displays XPS power budgeting, the allocated and budgeted power of all switches in the power stack. 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. Displays the configuration and status of all ports or the specified XPS port. Port numbers are from 1 to 9. Displays the status of the XPS power supplies. Displays the XPS system status. Displays the XPS thermal status. Displays the XPS upgrade status. Displays the XPS version details.
---------------------------	--	--

Command Modes	Privileged EXEC
----------------------	-----------------

Command History	Release	Modification
	12.2(55)SE1	This command was introduced.

Usage Guidelines	Use the show env xps privileged EXEC command to display the information for XPS 2200.
-------------------------	--

Examples	This is an example of output from the show env xps budgeting command:
-----------------	---

```
Switch#
=====

XPS 0101.0100.0000 :
=====
Data           Current   Power      Power Port  Switch #  PS A  PS B  Role-State
Committed
Budget
----- ----- ----- ----- ----- -----
223          1543      -       -       -       1      -      -      715  SP-PS
```

				SP-PS	223	223
2	-	-	-	-	-	-
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        -      -           -      -
```

show env xps

```

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 172: Related Commands

Command	Description
<code>power xps</code> (global configuration command)	Configures XPS and XPS port names.
<code>power xps</code> (privileged EXEC command)	Configures the XPS ports and system.

show flow monitor

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

Syntax Description	
name	(Optional) Specifies the name of a flow monitor.
<i>monitor-name</i>	(Optional) Name of a flow monitor that was previously configured.
cache	(Optional) Displays the contents of the cache for the flow monitor.
format	(Optional) Specifies the use of one of the format options for formatting the display output.
csv	(Optional) Displays the flow monitor cache contents in comma-separated variables (CSV) format.
record	(Optional) Displays the flow monitor cache contents in record format.
table	(Optional) Displays the flow monitor cache contents in table format.
statistics	(Optional) Displays the statistics for the flow monitor.

Command Modes	Privileged EXEC

show flow monitor

Command History

Release	Modification
Cisco IOS XE Everest 16.6.1	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 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 collects values as additional data for the cache.

Examples

The following example displays the status for a flow monitor:

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

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

This table describes the significant fields shown in the display.

Table 173: show flow monitor monitor-name Field Descriptions

Field	Description
Flow Monitor	Name of the flow monitor that you configured.
Description	Description that you configured or the monitor, or the default description User defined.
Flow Record	Flow record assigned to the flow monitor.
Flow Exporter	Exporters that are assigned to the flow monitor.
Cache	Information about the cache for the flow monitor.
Type	Flow monitor cache type. The value is always normal, as it is the only supported cache type.
Status	Status of the flow monitor cache. The possible values are: <ul style="list-style-type: none"> • allocated—The cache is allocated. • being deleted—The cache is being deleted. • not allocated—The cache is not allocated.

Field	Description
Size	Current cache size.
Inactive Timeout	Current value for the inactive timeout in seconds.
Active Timeout	Current value for the active timeout in seconds.

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

This table describes the significant fields shown in the display.

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

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

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

show install

To display information about install packages, use the **show install** command in privileged EXEC mode.

show install {active | committed | inactive | log | package {bootflash: | flash: | webui:} | rollback | summary | uncommitted}

Syntax Description	active	Displays information about active packages.
	committed	Displays package activations that are persistent.
	inactive	Displays inactive packages.
	log	Displays entries stored in the logging installation buffer.
	package	Displays metadata information about the package, including description, restart information, components in the package, and so on.
	{bootflash: flash: harddisk: webui:}	Specifies the location of the install package.
	rollback	Displays the software set associated with a saved installation.
	summary	Displays information about the list of active, inactive, committed, and superseded packages.
	uncommitted	Displays package activations that are nonpersistent.

Command Modes Privileged EXEC (#)

show install

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 174: 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	Install 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 all
Smart Licensing Status
=====
Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: CISCO Systems
  Virtual Account: NPR
  Export-Controlled Functionality: Not Allowed
  Initial Registration: SUCCEEDED on Jul 27 08:38:44 2018 EDT
  Last Renewal Attempt: None
  Next Renewal Attempt: Jan 23 08:38:44 2019 EDT
  Registration Expires: Jul 27 08:32:51 2019 EDT

License Authorization:
  Status: AUTHORIZED on Jul 27 08:38:49 2018 EDT
  Last Communication Attempt: SUCCEEDED on Jul 27 08:38:49 2018 EDT
  Next Communication Attempt: Aug 26 08:38:49 2018 EDT
  Communication Deadline: Oct 25 08:32:57 2018 EDT
```

show license all

```

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
=====
C9400 DNA Advantage (dna_advantage-C9400):
  Description: C9400 DNA Advantage
  Count: 1
  Version: 1.0
  Status: AUTHORIZED

C9400 Network Advantage (advantagek9-C9400):
  Description: C9400 Network Advantage
  Count: 2
  Version: 1.0
  Status: AUTHORIZED

Product Information
=====
UDI: PID:C9410R,SN:FXS2132Q0GU

HA UDI List:
  Active:PID:C9410R,SN:FXS2132Q0GU
  Standby:PID:C9410R,SN:FXS2132Q0GU

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:(rel15)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.

show license summary

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: Not Allowed
  Last Renewal Attempt: None
  Next Renewal Attempt: Jan 23 08:38:43 2019 EDT

License Authorization:
  Status: AUTHORIZED
  Last Communication Attempt: SUCCEEDED
  Next Communication Attempt: Aug 26 08:38:48 2018 EDT

License Usage:
  License          Entitlement tag          Count Status
  -----
  C9400 DNA Advantage (dna_advantage-C9400) 1 AUTHORIZED
  C9400 Network Advantage (advantagek9-C9400) 2 AUTHORIZED
```

Related Commands

Command	Description
show license all	Displays entitlements information.

Command	Description
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:C9410R,SN:FXS2132Q0GU

HA UDI List:
  Active:PID:C9410R,SN:FXS2132Q0GU
  Standby:PID:C9410R,SN:FXS2132Q0GU
```

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.

show location**Example**

This example shows a sample output from the **show license usage** command:

```
Device# show license usage
License Authorization:
  Status: AUTHORIZED on Jul 27 08:38:49 2018 EDT

C9400 DNA Advantage (dna_advantage-C9400):
  Description: C9400 DNA Advantage
  Count: 1
  Version: 1.0
  Status: AUTHORIZED

C9400 Network Advantage (advantagek9-C9400):
  Description: C9400 Network Advantage
  Count: 2
  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 <i>identifier-string</i>	Information identifier of the civic location, custom location, or geo-spatial location.
interface <i>type number</i>	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 Everest 16.6.1		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 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

show parser encrypt file status

Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Example

This example shows the output from the **show mac address-table move update** command:

```
Device# show mac address-table move update

Switch-ID : 010b.4630.1780
Dst mac-address : 0180.c200.0010
Vlans/Macs supported : 1023/8320
Default/Current settings: Rcv Off/On, Xmt Off/On
Max packets per min : Rcv 40, Xmt 60
Rcv packet count : 10
Rcv conforming packet count : 5
Rcv invalid packet count : 0
Rcv packet count this min : 0
Rcv threshold exceed count : 0
Rcv last sequence# this min : 0
Rcv last interface : Po2
Rcv last src-mac-address : 0003.fd6a.8701
Rcv last switch-ID : 0303.fd63.7600
Xmt packet count : 0
Xmt packet count this min : 0
Xmt threshold exceed count : 0
Xmt pak buf unavail cnt : 0
Xmt last interface : None
```

show 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 16.8.1a	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
8526A305B17DAD3CF8705BACFD51A2D55A333415CABC73DAFDEFD8777AA77F482EC4B
731A09826A41FB3EFFC46DC02FBA666534DBEC7DCC0C029298DB8462A70DBA26833C2A
1472D1F08D721BA941CB94A418E43803699174572A5759445B3564D8EAE57D64AE304
EE1D2A9C53E93E05B24A92387E261199CED8D8A0CE7134596FF8D2D6E6DA773757C70C
D3BA91C43A591268C248DF32658999276FB972153ABE823F0ACFE9F3B6F0AD1A00E257
4A4CC41C954015A59FB8FE
Platform: WS-C3650-12X48UZ
```

show platform sudi certificate

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 :
-----------------	--

```
Device# show platform sudi certificate

-----BEGIN CERTIFICATE-----
MIIDQzCCAiugAwIBAgIQX/h7KctU3I1CoxW1aMmt/zANBgkqhkiG9w0BAQUFADA1
MRYwFAYDVQQKEw1DaXNjbyBTeXN0ZW1zMRSwGQYDVQQDExJDaXNjbyBsb290IENB
IDIwNDgwHhcNMjAxNzEyWhcNMjkwNTE0MjAyNTQyWjA1MRYwFAYDVQQK
Ew1DaXNjbyBTeXN0ZW1zMRSwGQYDVQQDExJDaXNjbyBsb290IENBIDIwNDgwggEg
MA0GCSqGSIb3DQEBAQAA4IBDQAwggEAoIBAQCwmmrmrp68Kd6ficba0ZmKUeIhH
xmJVhEAyv8CrLqUccda8bnuoqrpu0hWISEWdovyD0My5jOAmaHBKeN8hF570YQXJ
FcjPFto1YYmUQ61EqDGyEJu5Tm8sUxJszR2tKyS7McQr/4NEb7Y9JHcJ6r8qqB9q
VvYgDxFU14F1pyXOWWqCZe+36ufijXWLbvLdT6ZeYpzPEApk0E5tzivMW/VgpSdH
jWn0f84bcN5wGyDWbs2mAag8EtKpP6BrXruOII6ke0laO6g58QBdKhTCytKmg91
Eg6CTY5j/e/rmxrbU6YTYK/CfdfHbBcl1HP7R2RQgYCUTOG/rksc35LtLgXfAgED
o1EwTzALBgNVHQ8EBAMCAYwDwYDVR0TAQH/BAuAwEB/zAdBgNVHQ4EFgQUJ/PI
FR5umgIJFq0roIlgX9p7L6owEAYJKwYBBAGCNxUBBAMCAQAwDQYJKoZIhvNAQEF
BQADggEBAJ2dhISjQa18dw3U8pORFBi71R803UXHOjgxkhLtv5MohmBVrBW7hmW
Ycpao2TB9k5UM8Z3/sUcuuVdJcr18JOagxEu5sv4dEX+5wW4q+f fy0vhN4TauYuX
cB7w4ovXsNgOnbFp1iqRe61JT37mjpxYgycc81WhJdtSd9i7rp77rMKSSh0T81asz
Bvt9YAreTIpjsJyp8qS5UwGH0GikJ3+r/+n6yUA4iGe0OcaEb1fJU9u6ju7AQ7L4
CYNu/2bPPu8Xs1gYJQk0XuPL1s2PKSb3TkL4Eq1ZKR4OCXPJDJoBYVL0fdX41Id
kxpUnwVwwEpxYB5DC2Ae/qPOgRnhCzU=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEPDCCAySgAwIBAgIKYQlufQAAAAADDANBgkqhkiG9w0BAQUFADA1MRYwFAYD
VQQKEw1DaXNjbyBTeXN0ZW1zMRSwGQYDVQQDExJDaXNjbyBsb290IENBIDIwNDgw
HhcNMTEwNjMwMTc1NjU3WhcNMjkwNTE0MjAyNTQyWjA1MQR4wDAYDVQQKEwVDaXNj
bzEVMBMGA1UEAxMMQUNUMiBTURJIENBMIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEA0m513THIxA9tN/hS5qR/6U2Rpdd+9aE2JbFkNjht6gfHKd477Aks
5XAtUs5oxDYvt/zEbs1Zq3+LR6qrqKKQVu6JYvH05UYLBqCj38s76NLk53905Wzp
9pRcmRCpUX+a6tHF/qRuOjJ44mdeDYzo3qPCpxzprWJDPclM4iYKHumMQmqmrg+
xghHioWS80BOcdiynebeP5rZ7qRuewKMpl1T3WdBNjZjnpfjg66F+p4SaDkGb
BXdgj13oVeF+EywFLrFjj97fL2+8oauV43Qrvnf3d/GfqXj7ew+z/sX1XtEOjSXJ
URsyMEj53Rdd9tJwHky8neapszs+r+kdVQIDAQABo4IBWjCCAVYwCwYDVR0PBQD
AgHGMB0GA1UdIgQWBRI2PHxwnDVW7t8cwmTr7i4MAP4FzAfBgNVHSMEGDAwBQn
88gVHm6aAgkWrSugiWBF2nsvqjBDBgNVHR8EPDA6MDigNqA0hjJodHRwOi8vd3d3
LmNpc2NvLmNbS9zZWN1cmloes9wa2kvY3JsL2NyY2EyMDQ4LmNybDBQBgrBgfEF
-----END CERTIFICATE-----
```

```
BQcBAQREMEIwQAYIKwYBBQUHMAKGNGh0dHA6Ly93d3cuY21zY28uY29tL3N1Y3VyaXRS9jZXJ0cy9jcmNhMjA0OC5jZXIwXAYDVR0gBFUwUzBRBgorBgeEAQkVAQwAMEMwQQYIKwYBBQUHAgEWNWh0dHA6Ly93d3cuY21zY28uY29tL3N1Y3VyaXR5L3Bras9wb2xpY211cy9pbmR1eC5odG1sMBIGA1UdEwEB/wQIMAYBAf8CAQAwDQYJKoZIhvcNAQEfbQADggEBAGh1qclr9tx4hzWgDERm371yeuEmqcIfi9b9+GbMSJbiZHc/Ccc101Ju0a9zTXA9w47H9/t61eduGxb4WeLxwcCiUgvFtcA51Iklt8nNbckY/4dw1ex+7amATUQO4QggIE67wVIPu6bgAE3Ja/nRS3xKYSnj8H5TehimBSv6TECi5jUhOWryAK4dvo8hCjkjEkzu3ufBTJapnv89g9OE+H3VKM4L+/KdkUO+52djFKnhy147d7cZR4DY4LIuFM2P1As8YyjzoNPK/urSRI14Wd1lplR1nH7KND15618yfVP0IFJZBGrooCRBjOSwFv8cpWCbmWdPaCQT2nwIjTfy8c=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDhjCCAm6gAwIBAgIDctWkMA0GCSqGSIb3DQEBCwUAMCcxDjAMBgNVBAotBUNpc2NvMRUwEwYDVQQDEwxBQ1QyIFNVREkgQ0EwHhcNMTUwODA2MDgwODI5WhcNMjUwODA2MDgwODI5WjBzMswkYgYDVQQFEyNQSUQ6V1MtQzM2NTAtMTJYNDhVWiBTTjpGRE8xOTMyWDawQzEOMAwGA1UEChMFQ21zY28xGDAWBgNVBAsTD0FDVC0yIEpdGUgU1VESTEZMBcGA1UEAxMQV1MtQzM2NTAtMTJYNDhVWjCCASiWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBANzXOGYI0eU14HcSwjL4HO75qTj19C2BHg3ufce9ikkNkwGXj8qg8vKxuB9tRYRaJC5bP1WMoq7+ZjtQA079xE4X14soNbq5NaUh7RB1wDjRUJvTfCOzVICbNfbzvtB30I75tCarFNmpd0K6AFrIa41U988QGqaCj7R1JrYNajnC73UXXM/hC0HtNR5myqer5Y2qjjzo6tHZYqrrx2eS1XoA262ZSQriAxmaH/KLC97ywyRBdJ1xBRX3hGtKlog8nASB8WpxqB9NCERzUajwU3L/kg2BsCqw9Y2m7HWU1cerTxgthuyUkdNI+Jg6iGApn2+s8E9hsHPBPMcdIsCAwEAAaNvMG0wDgYDVR0PAQH/BAQDAgXgMAwGA1UdEwEB/wQCMAAwTQYDVR0RBElYwRKBCBgkrBgeEAQkVAgOgNRMzQ2hpCE1EPVVZSk5ORmRR1FvN1ZIVmxJRTlqZENBeU9DQXhPRG93T1RveE1TQVg5eWc9MA0GCSqGSIb3DQEBCwUAA4IBAQBKicTRzbvCRjVIR5MqcWXUT086v6EjHahDHTs3YpQoyAVfioNg2x8J6EXcEau4voyVu+eMuuoNL4szPhmmDcULfiCGBcAR3EFuoVMIzNT0geziytsCf728KGw1oGuosgVjNGOOahUELu4+F/My7bIJNbH+PDkjIFmhJpJg0F3q17yClAeXvd13g3W39i35d00Lm5L1WbBfQtyBaOLAbxsHvutrxu1VZ5sdqSTwTkk09vKMaQjh7a8J/AmJi93jvzM69pe5711P1zqZfYfpiJ3cyJ0xfI4brQ1smdczloFD4asF7a+1vor5e4VDBP0ppmeFAJvCQ52JTpj0M0c1D
-----END CERTIFICATE-----
```

show sdm prefer

To display information about the templates that can be used to maximize system resources for a particular feature, use the **show sdm prefer** command in privileged EXEC mode. To display the current template, use the command without a keyword.

show sdm prefer [advanced]

Syntax Description	advanced (Optional) Displays information on the advanced template.				
Command Default	No default behavior or values.				
Command Modes	Privileged EXEC				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				

show tech-support license**Usage Guidelines**

If you did not reload the switch after entering the **sdm prefer** global configuration command, the **show sdm prefer** privileged EXEC command displays the template currently in use and not the newly configured template.

The numbers displayed for each template represent an approximate maximum number for each feature resource. The actual number might vary, depending on the actual number of other features configured. For example, in the default template if your device had more than 16 routed interfaces (subnet VLANs), the number of possible unicast MAC addresses might be less than 6000.

Example

The following is sample output from the **show sdm prefer** command:

```
Device# show sdm prefer

Showing SDM Template Info

This is the Advanced template.

Number of VLANs: 4094
Unicast MAC addresses: 32768
Overflow Unicast MAC addresses: 512
IGMP and Multicast groups: 8192
Overflow IGMP and Multicast groups: 512
Directly connected routes: 32768
Indirect routes: 7680
Security Access Control Entries: 3072
QoS Access Control Entries: 3072
Policy Based Routing ACEs: 1024
Netflow ACEs: 1024
Input Microflow policer ACEs: 256
Output Microflow policer ACEs: 256
Flow SPAN ACEs: 256
Tunnels: 256
Control Plane Entries: 512
Input Netflow flows: 8192
Output Netflow flows: 16384
SGT/DGT entries: 4096
SGT/DGT Overflow entries: 512

These numbers are typical for L2 and IPv4 features.
Some features such as IPv6, use up double the entry size;
so only half as many entries can be created.

Device#
```

show tech-support 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 mcpred

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.
	show license summary	Displays summary of all active licenses.
	show license udi	Displays UDI.
	show license usage	Displays license usage information

test cable-diagnostic tdr

To run the Time Domain Reflector (TDR) feature on an interface, use the **test cable-diagnostic tdr** command in privileged EXEC mode.

test cable-diagnostics tdr interface *interface-id*

Syntax Description	<i>interface-id</i> The interface on which to run TDR.
---------------------------	--

Command Default	No default behavior or values.
------------------------	--------------------------------

Command Modes	Privileged EXEC
----------------------	-----------------

Command History	Release	Modification
Cisco IOS XE Everest 16.6.1		This command was introduced.

Usage Guidelines	TDR is supported only on 10/100/100 copper Ethernet ports. It is not supported on 10-Gigabit Ethernet ports or small form-factor pluggable (SFP) module ports.
-------------------------	--

After you run TDR by using the **test cable-diagnostics tdr interface *interface-id*** command, use the **show cable-diagnostics tdr interface *interface-id*** privileged EXEC command to display the results.

This example shows how to run TDR on an interface:

```
Device# test cable-diagnostics tdr interface gigabitethernet1/0/2
TDR test started on interface Gi1/0/2
A TDR test can take a few seconds to run on an interface
Use 'show cable-diagnostics tdr' to read the TDR results
```

If you enter the **test cable-diagnostics tdr interface *interface-id*** command on an interface that has an link up status and a speed of 10 or 100 Mb/s, these messages appear:

```
Device# test cable-diagnostics tdr interface gigabitethernet1/0/3
TDR test on Gi1/0/9 will affect link state and traffic
TDR test started on interface Gi1/0/3
A TDR test can take a few seconds to run on an interface
Use 'show cable-diagnostics tdr' to read the TDR results.
```

traceroute mac

To display the Layer 2 path taken by the packets from the specified source MAC address to the specified destination MAC address, use the **traceroute mac** command in privileged EXEC mode.

**traceroute mac [interface *interface-id*] *source-mac-address* [interface *interface-id*]
destination-mac-address [vlan *vlan-id*] [detail]**

Syntax Description	<i>interface interface-id</i> (Optional) Specifies an interface on the source or destination device.
<i>source-mac-address</i>	The MAC address of the source device in hexadecimal format.
<i>destination-mac-address</i>	The MAC address of the destination device in hexadecimal format.

vlan *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 Everest 16.6.1		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
```

traceroute mac

```
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed
```

This example shows how to display the Layer 2 path by using the **detail** keyword:

```
Device# traceroute mac 0000.0201.0601 0000.0201.0201 detail
Source 0000.0201.0601 found on con6[WS-C3750E-24PD] (2.2.6.6)
con6 / WS-C3750E-24PD / 2.2.6.6 :
    Gi0/0/2 [auto, auto] => Gi0/0/3 [auto, auto]
con5 / WS-C2950G-24-EI / 2.2.5.5 :
    Fa0/3 [auto, auto] => Gi0/1 [auto, auto]
con1 / WS-C3550-12G / 2.2.1.1 :
    Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2 / WS-C3550-24 / 2.2.2.2 :
    Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
```

This example shows how to display the Layer 2 path by specifying the interfaces on the source and destination devicees:

```
Device# traceroute mac interface fastethernet0/1 0000.0201.0601 interface fastethernet0/3
0000.0201.0201
Source 0000.0201.0601 found on con6[WS-C3750E-24PD] (2.2.6.6)
con6 (2.2.6.6) :Gi0/0/1 => Gi0/0/3
con5 (2.2.5.5) : Gi0/0/3 => Gi0/0/1
con1 (2.2.1.1) : Gi0/0/1 => Gi0/0/2
con2 (2.2.2.2) : Gi0/0/2 => Gi0/0/1
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed
```

This example shows the Layer 2 path when the device is not connected to the source device:

```
Device# traceroute mac 0000.0201.0501 0000.0201.0201 detail
Source not directly connected, tracing source .....
Source 0000.0201.0501 found on con5[WS-C3750E-24TD] (2.2.5.5)
con5 / WS-C3750E-24TD / 2.2.5.5 :
    Gi0/0/1 [auto, auto] => Gi0/0/3 [auto, auto]
con1 / WS-C3550-12G / 2.2.1.1 :
    Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2 / WS-C3550-24 / 2.2.2.2 :
    Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
```

This example shows the Layer 2 path when the device cannot find the destination port for the source MAC address:

```
Device# traceroute mac 0000.0011.1111 0000.0201.0201
Error:Source Mac address not found.
Layer2 trace aborted.
```

This example shows the Layer 2 path when the source and destination devices are in different VLANs:

```
Device# traceroute mac 0000.0201.0601 0000.0301.0201
      Error:Source and destination macs are on different vlans.
      Layer2 trace aborted.
```

This example shows the Layer 2 path when the destination MAC address is a multicast address:

```
Device# traceroute mac 0000.0201.0601 0100.0201.0201
      Invalid destination mac address
```

This example shows the Layer 2 path when source and destination devicees belong to multiple VLANs:

```
Device# traceroute mac 0000.0201.0601 0000.0201.0201
      Error:Mac found on multiple vlans.
      Layer2 trace aborted.
```

traceroute mac ip

To display the Layer 2 path taken by the packets from the specified source IP address or hostname to the specified destination IP address or hostname, use the **traceroute mac ip** command in privileged EXEC mode.

traceroute mac ip {source-ip-address source-hostname} {destination-ip-address destination-hostname} [detail]

Syntax Description	<p><i>source-ip-address</i> The IP address of the source device as a 32-bit quantity in dotted-decimal format.</p> <p><i>source-hostname</i> The IP hostname of the source device.</p> <p><i>destination-ip-address</i> The IP address of the destination device as a 32-bit quantity in dotted-decimal format.</p> <p><i>destination-hostname</i> The IP hostname of the destination device.</p> <p>detail (Optional) Specifies that detailed information appears.</p>				
Command Default	No default behavior or values.				
Command Modes	Privileged EXEC				
Command History	<table border="1"> <thead> <tr> <th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td><td>This command was introduced.</td></tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				

traceroute mac ip**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	<i>filesystem:</i> Alias for a file system. Use flash: for the system board flash device; use usbflash0: for USB memory sticks. <i>/file-url...</i> Path (directory) and name of the files to display. Separate each filename with a space.				
Command Default	No default behavior or values.				
Command Modes	Boot loader				
Command History	<table border="1"> <thead> <tr> <th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td><td>This command was introduced.</td></tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	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

```

unset

```
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	<p><i>variable</i> Use one of these keywords for <i>variable</i>:</p> <p>MANUAL_BOOT—Specifies whether the device automatically or manually boots.</p>				
	<p>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.</p>				
	<p>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.</p>				
	<p>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.</p>				
	<p>PS1—Specifies the string that is used as the command-line prompt in boot loader mode.</p>				
	<p>CONFIG_FILE—Resets the filename that Cisco IOS uses to read and write a nonvolatile copy of the system configuration.</p>				
	<p>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.</p>				
Command Default	No default behavior or values.				
Command Modes	Boot loader				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				
Usage Guidelines	Under typical circumstances, it is not necessary to alter the setting of the environment variables.				

The MANUAL_BOOT environment variable can also be reset by using the **no boot manual** global configuration command.

The BOOT environment variable can also be reset by using the **no boot system** global configuration command.

The ENABLE_BREAK environment variable can also be reset by using the **no boot enable-break** global configuration command.

The HELPER environment variable can also be reset by using the **no boot helper** global configuration command.

The CONFIG_FILE environment variable can also be reset by using the **no boot config-file** global configuration command.

Example

This example shows how to unset the SWITCH_PRIORITY environment variable:

```
Device: unset SWITCH_PRIORITY
```

version

To display the boot loader version, use the **version** command in boot loader mode.

version

Syntax Description This command has no arguments or keywords.

Command Default No default behavior or values.

Command Modes Boot loader

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Examples This example shows how to display the boot loader version on a device:

CHAPTER 22

Tracing

- [Information About Tracing, on page 1095](#)
- [set platform software trace, on page 1097](#)
- [show platform software trace filter-binary, on page 1101](#)
- [show platform software trace message, on page 1101](#)
- [show platform software trace level, on page 1104](#)
- [request platform software trace archive, on page 1107](#)
- [request platform software trace rotate all, on page 1108](#)
- [request platform software trace filter-binary, on page 1108](#)

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
- /hddisk/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 175: 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*

set platform software trace

Syntax Description	<i>process</i>	Process whose tracing level is being set. Options include:
		<ul style="list-style-type: none">• chassis-manager—The Chassis Manager process.• cli-agent—The CLI Agent process.• dbm—The Database Manager process.• emd—The Environmental Monitoring process.• fed—The Forwarding Engine Driver process.• forwarding-manager—The Forwarding Manager process.• host-manager—The Host Manager process.• iomd—The Input/Output Module daemon (IOMd) process.• ios—The IOS process.• license-manager—The License Manager process.• logger—The Logging Manager process.• platform-mgr—The Platform Manager process.• pluggable-services—The Pluggable Services process.• replication-mgr—The Replication Manager process.• shell-manager—The Shell Manager process.• smd—The Session Manager process.• table-manager—The Table Manager Server.• wireshark—The Embedded Packet Capture (EPC) Wireshark process.

<i>slot</i>	Hardware slot where the process for which the trace level is set, is running. Options include: <ul style="list-style-type: none">• <i>number</i>—Number of the SIP slot of the hardware module where the trace level is set. For instance, if you want to specify the SIP in SIP slot 2 of the switch, enter 2.• <i>SIP-slot / SPA-bay</i>—Number of the SIP switch slot and the number of the shared port adapter (SPA) bay of that SIP. For instance, if you want to specify the SPA in bay 2 of the SIP in switch slot 3, enter 3/2.• F0—The Embedded-Service-Processor in slot 0.• FP active—The active Embedded-Service-Processor.• R0—The route processor in slot 0.• RP active—The active route processor.• switch <number>—The switch with its number specified.• switch active—The active switch.• switch standby—The standby switch.
-------------	---

<i>module</i>	Module within the process for which the tracing level is set.
---------------	---

set platform software trace*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 DefaultThe default tracing level for all modules is **notice**.**Command Modes**

User EXEC (>)

Privileged EXEC (#)

Command History**Release****Modification**

Cisco IOS XE Everest 16.6.2 This command was introduced.

Usage Guidelines

The *module* options vary by process and by *hardware-module*. Use the ? option when entering this command to see which *module* options are available with each keyword sequence.

Use the **show platform software trace message** command to view trace messages.

Trace files are stored in the *tracelogs* directory in the *harddisk: file system*. These files can be deleted without doing any harm to your switch operation.

Trace file output is used for debugging. The trace level is a setting that determines how much information should be stored in trace files about a module.

Examples

This example shows how to set the trace level for all the modules in dbm process:

```
Device# set platform software trace dbm R0 all-modules debug
```

show platform software trace filter-binary

To display the most recent trace information for a specific module, use the **show platform software trace filter-binary** command in privileged EXEC or user EXEC mode.

```
show platform software trace filter-binary [context mac-address]
```

Syntax Description	context <i>mac-address</i>	Represents the context used to filter. Additionally, you can filter based on module names and trace levels. The context keyword accepts either a MAC address or any other argument based on which a trace is tagged.
Command Modes	User EXEC (> Privileged EXEC (#)	
Command History	Release Cisco IOS XE Everest 16.6.2	Modification This command was introduced.
Usage Guidelines	This command collates and sorts all the logs present in the <code>/tmp/...</code> across all the processes relevant to the module. The trace logs of all the processes relevant to the specified module are printed to the console. This command also generates a file named <code>collated_log_{system time}</code> with the same content, in the <code>/crashinfo/tracelogs</code> 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
```

show platform software trace message

Syntax Description	<i>process</i>	Tracing level that is being set. Options include: <ul style="list-style-type: none">• chassis-manager—The Chassis Manager process.• cli-agent—The CLI Agent process.• cmm—The CMM process.• dbm—The Database Manager process.• emd—The Environmental Monitoring process.• fed—The Forwarding Engine Driver process.• forwarding-manager—The Forwarding Manager process.• geo—The Geo Manager process.• host-manager—The Host Manager process.• interface-manager—The Interface Manager process.• iomd—The Input/Output Module daemon (IOMd) process.• ios—The IOS process.• license-manager—The License Manager process.• logger—The Logging Manager process.• platform-mgr—The Platform Manager process.• pluggable-services—The Pluggable Services process.• replication-mgr—The Replication Manager process.• shell-manager—The Shell Manager process.• sif—The Stack Interface (SIF) Manager process.• smd—The Session Manager process.• stack-mgr—The Stack Manager process.• table-manager—The Table Manager Server.• thread-test—The Multithread Manager process.• virt-manager—The Virtualization Manager process.
--------------------	----------------	---

<i>slot</i>	<p>Hardware slot where the process for which the trace level is set, is running. Options include:</p> <ul style="list-style-type: none"> • <i>number</i>—Number of the SIP slot of the hardware module where the trace level is set. For instance, if you want to specify the SIP in SIP slot 2 of the switch, enter 2. • <i>SIP-slot / SPA-bay</i>—Number of the SIP switch slot and the number of the shared port adapter (SPA) bay of that SIP. For instance, if you want to specify the SPA in bay 2 of the SIP in switch slot 3, enter 3/2. • F0—The Embedded Service Processor 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. <ul style="list-style-type: none"> • <i>number</i>—Number of the SIP slot of the hardware module where the trace level is set. For instance, if you want to specify the SIP in SIP slot 2 of the switch, enter 2. • <i>SIP-slot / SPA-bay</i>—Number of the SIP switch slot and the number of the shared port adapter (SPA) bay of that SIP. For instance, if you want to specify the SPA in bay 2 of the SIP in switch slot 3, enter 3/2. • F0—The Embedded Service Processor in slot 0. • FP active—The active Embedded Service Processor. • R0—The route processor in slot 0. • RP active—The active route processor.
-------------	--

Command Modes	User EXEC (>)
----------------------	---------------

Privileged EXEC (#)

Command History	Release	Modification
------------------------	----------------	---------------------

Cisco IOS XE Everest 16.6.2 This command was introduced.

show platform software trace level

Examples

This example shows how to display the trace messages for the Stack Manager and the Forwarding Engine Driver processes:

```
Device# show platform software trace message stack-mgr switch active R0
10/30 09:42:48.767 [btrace] [8974]: (note): Successfully registered module [97] [uiutil]
10/30 09:42:48.762 [btrace] [8974]: (note): Successfully registered module [98]
[tdl_cdlcore_message]
10/29 13:28:19.023 [stack_mgr] [8974]: (note): Examining peer state
10/29 13:28:19.023 [stack_mgr] [8974]: (note): no switch eligible for standby election
presently
10/29 13:28:19.022 [stack_mgr] [8974]: (note): Posting event
stack_fsm_event_wait_standby_elect_timer_expired, curstate stack_fsm_state_active_ready
10/29 13:28:19.022 [stack_mgr] [8974]: (note): Timer HDL - STACK_WAIT_STANDBY_ELECT_TIMER
expired
10/29 13:26:46.584 [btrace] [8974]: (note): Successfully registered module [99]
[tdl_ui_message]
10/29 13:26:46.582 [bipc] [8974]: (note): Pending connection to server 10.129.1.0
10/29 13:26:36.582 [evutil] [8974]: (ERR): Connection attempt for sman-ui-serv (uipeer
uplink to slot 1) failed, invoking disconnect
10/29 13:26:36.582 [evutil] [8974]: (ERR): Asynchronous connect failed for [uipeer uplink
to slot 1] (fd == -1)
10/29 13:26:36.581 [bipc] [8974]: (note): Pending connection to server 10.129.1.0
10/29 13:26:26.581 [evutil] [8974]: (ERR): Connection attempt for sman-ui-serv (uipeer
uplink to slot 1) failed, invoking disconnect

Device# show platform software trace message fed switch active
11/02 10:55:01.832 [btrace]: [11310]: UUID: 0, ra: 0 (note): Successfully registered module
[86] [uiutil]
11/02 10:55:01.848 [btrace]: [11310]: UUID: 0, ra: 0 (note): Single message size is greater
than 1024
11/02 10:55:01.822 [btrace]: [11310]: UUID: 0, ra: 0 (note): Successfully registered module
[87] [tdl_cdlcore_message]
11/01 09:54:41.474 [btrace]: [12312]: UUID: 0, ra: 0 (note): Successfully registered module
[88] [tdl_ngwc_gold_message]
11/01 09:54:11.228 [btrace]: [12312]: UUID: 0, ra: 0 (note): Successfully registered module
[89] [tdl_doppler_iosd_matm_type]
11/01 09:53:37.454 [btrace]: [11310]: UUID: 0, ra: 0 (note): Successfully registered module
[90] [tdl_ui_message]
11/01 09:53:37.382 [bipc]: [11310]: UUID: 0, ra: 0 (note): Pending connection to server
10.129.1.0
11/01 09:53:34.227 [xcvr]: [18846]: UUID: 0, ra: 0 (ERR): FRU hardware authentication Fail,
result = 1.
11/01 09:53:33.775 [ng3k_scc]: [18846]: UUID: 0, ra: 0 (ERR): SMART COOKIE: SCC I2C receive
failed: rc=10
11/01 09:53:33.775 [ng3k_scc]: [18846]: UUID: 0, ra: 0 (ERR):
SMART COOKIE receive failed, try again
11/01 09:53:33.585 [ng3k_scc]: [18846]: UUID: 0, ra: 0 (ERR):
```

show platform software trace level

To view the trace levels for all the modules under a specific process, use the **show platform software trace level** command in privileged EXEC or user EXEC mode.

show platform software trace level *process slot*

Syntax Description	<i>process</i>	Process whose tracing level is being set. Options include:
		<ul style="list-style-type: none">• 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.

show platform software trace level

<i>slot</i>	<p>Hardware slot where the process for which the trace level is set, is running. Options include:</p> <ul style="list-style-type: none"> • <i>number</i>—Number of the SIP slot of the hardware module where the trace level is set. For instance, if you want to specify the SIP in SIP slot 2 of the switch, enter 2. • <i>SIP-slot / SPA-bay</i>—Number of the SIP switch slot and the number of the shared port adapter (SPA) bay of that SIP. For instance, if you want to specify the SPA in bay 2 of the SIP in switch slot 3, enter 3/2. • F0—The Embedded Service Processor in slot 0. • F1—The Embedded Service Processor in slot 1. • FP active—The active Embedded Service Processor. • R0—The route processor in slot 0. • RP active—The active route processor. • switch <number>—The switch, with its number specified. • switch active—The active switch. • switch standby—The standby switch. • <i>number</i>—Number of the SIP slot of the hardware module where the trace level is set. For instance, if you want to specify the SIP in SIP slot 2 of the switch, enter 2. • <i>SIP-slot / SPA-bay</i>—Number of the SIP switch slot and the number of the shared port adapter (SPA) bay of that SIP. For instance, if you want to specify the SPA in bay 2 of the SIP in switch slot 3, enter 3/2. • F0—The Embedded Service Processor in slot 0. • FP active—The active Embedded Service Processor. • R0—The route processor in slot 0. • RP active—The active route processor.
-------------	--

Command Modes User EXEC (>)

Privileged EXEC (#)

Command History **Release** **Modification**

Cisco IOS XE Everest 16.6.2 This command was introduced.

Examples This example shows how to view the trace level:

```
Device# show platform software trace level dbm switch active R0
```

Module Name	Trace Level
<hr/>	
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 <i>number-of-days</i>	Specifies the number of days for which the trace files have to be archived.
	target <i>location</i>	Specifies the location and name of the archive file.

Command Modes User EXEC (>)

Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.2	This command was introduced.

Usage Guidelines This archive file can be copied from the system, using the tftp or scp commands.

Examples This example shows how to archive all the trace logs of the processes running on the switch since the last 5 days:

```
Device# request platform software trace archive last 5 days target flash:test_archive
```

request platform software trace rotate all

request platform software trace rotate all

To rotate all the current in-memory trace logs into the crashinfo partition and start a new in-memory trace log for each process, use the **request platform software trace rotate all** command in privileged EXEC or user EXEC mode.

request platform software trace rotate all

Command Modes	User EXEC (>) Privileged EXEC (#)				
Command History	<table border="1"> <thead> <tr> <th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.2</td><td>This command was introduced.</td></tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.2	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.2	This command was introduced.				
Usage Guidelines	The trace log files are for read-only purpose. Do not edit the contents of the file. If there is a requirement to delete the contents of the file to view certain set of logs, use this command to start a new trace log file.				
Examples	This example shows how to rotate all the in-memory trace logs of the processes running on the switch since the last one day:				

```
Device# request platform software trace slot switch active R0 archive last 1 days target
flash:test
```

request platform software trace filter-binary

To collate and sort all the archived logs present in the tracelogs subdirectory, use the **request platform software trace filter-binary** command in privileged EXEC or user EXEC mode.

request platform software trace filter-binary *modules* [**context** *mac-address*]

Syntax Description	context <i>mac-address</i>	Represents the context used to filter. Additionally, you can filter based on module names and trace levels. The context keyword accepts either a MAC address or any other argument based on which a trace is tagged.				
Command Modes	User EXEC (>) Privileged EXEC (#)					
Command History	<table border="1"> <thead> <tr> <th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.2</td><td>This command was introduced.</td></tr> </tbody> </table>		Release	Modification	Cisco IOS XE Everest 16.6.2	This command was introduced.
Release	Modification					
Cisco IOS XE Everest 16.6.2	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.

request platform software trace filter-binary



PART **XIV**

VLAN

- [VLAN Commands, on page 1113](#)

VLAN Commands

- [clear vtp counters, on page 1113](#)
- [debug platform vlan, on page 1114](#)
- [debug sw-vlan, on page 1114](#)
- [debug sw-vlan ifs, on page 1115](#)
- [debug sw-vlan notification, on page 1116](#)
- [debug sw-vlan vtp, on page 1117](#)
- [interface vlan, on page 1118](#)
- [show platform vlan, on page 1119](#)
- [show vlan, on page 1119](#)
- [show vtp, on page 1122](#)
- [switchport priority extend, on page 1127](#)
- [switchport trunk, on page 1128](#)
- [vlan, on page 1130](#)
- [vtp \(global configuration\), on page 1136](#)
- [vtp \(interface configuration\), on page 1140](#)
- [vtp primary, on page 1141](#)

clear vtp counters

To clear the VLAN Trunking Protocol (VTP) and pruning counters, use the **clear vtp counters** command in privileged EXEC mode.

clear vtp counters

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Privileged EXEC

Command History	Release	Modification
Cisco IOS XE Everest 16.6.1		This command was introduced.

debug platform vlan

This example shows how to clear the VTP counters:

```
Device# clear vtp counters
```

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

debug platform vlan

To enable debugging of the VLAN manager software, use the **debug platform vlan** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

Command Default	Debugging is disabled.				
Command Modes	Privileged EXEC				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				
Usage Guidelines	The undebbug platform vlan command is the same as the no debug platform vlan command.				

This example shows how to display VLAN error debug messages:

```
Device# debug platform vlan error
```

debug sw-vlan

To enable debugging of VLAN manager activities, use the **debug sw-vlan** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

```
debug sw-vlan {badpmcookies | cfg-vlan {bootup | cli} | events | ifs | mapping | notification | packets |
redundancy | registries | vtp}
no debug sw-vlan {badpmcookies | cfg-vlan {bootup | cli} | events | ifs | mapping | notification | packets |
redundancy | registries | vtp}
```

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 1115 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 1116 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 1117 for more information.

Command Default Debugging is disabled.

Command Modes Privileged EXEC

Command History	Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced.	

Usage Guidelines The **undebbug sw-vlan** command is the same as the **no debug sw-vlan** command.

This example shows how to display debug messages for VLAN manager events:

```
Device# 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	Displays VLAN manager IFS file-read operation debug messages.
read	

open	Displays VLAN manager IFS file-write operation debug messages.
write	

read	Displays file-read operation debug messages for the specified error test (1 , 2 , 3 , or 4).
-------------	--

write	Displays file-write operation debug messages.
--------------	---

debug sw-vlan notification

Command Default	Debugging is disabled.				
Command Modes	Privileged EXEC				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td><td>This command was introduced.</td></tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	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.

This example shows how to display file-write operation debug messages:

```
Device# debug sw-vlan ifs write
```

debug sw-vlan notification

To enable debugging of VLAN manager notifications, use the **debug sw-vlan notification** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

```
debug sw-vlan notification {accfwdchange | allowedvlancfgchange | fwdchange | linkchange | modechange | pruningcfgchange | statechange}
no debug sw-vlan notification {accfwdchange | allowedvlancfgchange | fwdchange | linkchange | modechange | pruningcfgchange | statechange}
```

Syntax Description	accfwdchange	Displays debug messages for VLAN manager notification of aggregated access interface spanning-tree forward changes.
	allowedvlancfgchange	Displays debug messages for VLAN manager notification of changes to the allowed VLAN configuration.
	fwdchange	Displays debug messages for VLAN manager notification of spanning-tree forwarding changes.
	linkchange	Displays debug messages for VLAN manager notification of interface link-state changes.
	modechange	Displays debug messages for VLAN manager notification of interface mode changes.
	pruningcfgchange	Displays debug messages for VLAN manager notification of changes to the pruning configuration.
	statechange	Displays debug messages for VLAN manager notification of interface state changes.

Command Default Debugging is disabled.

Command Modes Privileged EXEC

Command History	Release	Modification
Cisco IOS XE Everest 16.6.1		This command was introduced.

Usage Guidelines The **undebbug sw-vlan notification** command is the same as the **no debug sw-vlan notification** command.

This example shows how to display debug messages for VLAN manager notification of interface mode changes:

```
Device# 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.

interface vlan

Command Modes	Privileged EXEC	
Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1 This command was introduced.	
Usage Guidelines	<p>The undebbug sw-vlan vtp command is the same as the no debug sw-vlan vtp command.</p> <p>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.</p>	

This example shows how to display debug messages for VTP redundancy:

```
Device# debug sw-vlan vtp redundancy
```

interface vlan

To create or access a dynamic switch virtual interface (SVI) and to enter interface configuration mode, use the **interface vlan** command in global configuration mode. To delete an SVI, use the **no** form of this command.

interface vlan *vlan-id*
no interface vlan *vlan-id*

Syntax Description	<i>vlan-id</i>	VLAN number. The range is 1 to 4094.
Command Default	The default VLAN interface is VLAN 1.	
Command Modes	Global configuration	
Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1 This command was introduced.	
Usage Guidelines	<p>SVIs are created the first time you enter the interface vlan <i>vlan-id</i> command for a particular VLAN. The <i>vlan-id</i> corresponds to the VLAN-tag associated with data frames on an IEEE 802.1Q encapsulated trunk or the VLAN ID configured for an access port.</p> <p>Note When you create an SVI, it does not become active until it is associated with a physical port.</p>	
	<p>If you delete an SVI using the no interface vlan <i>vlan-id</i> command, it is no longer visible in the output from the show interfaces privileged EXEC command.</p>	

**Note**

You cannot delete the VLAN 1 interface.

You can reinstate a deleted SVI by entering the **interface vlan *vlan-id*** command for the deleted interface. The interface comes back up, but the previous configuration is gone.

The interrelationship between the number of SVIs configured on a switch or a switch stack and the number of other features being configured might have an impact on CPU utilization due to hardware limitations. You can use the **sdm prefer** global configuration command to reallocate system hardware resources based on templates and feature tables.

You can verify your setting by entering the **show interfaces** and **show interfaces vlan *vlan-id*** privileged EXEC commands.

This example shows how to create a new SVI with VLAN ID 23 and enter interface configuration mode:

```
Device(config)# interface vlan 23
Device(config-if)#

```

show platform vlan

To display platform-dependent VLAN information, use the **show platform vlan** privileged EXEC command.

Command Default	None				
Command Modes	Privileged EXEC				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	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 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 | 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.

show vlan

id <i>vlan-id</i>	(Optional) Displays information about a single VLAN identified by the VLAN ID number. For <i>vlan-id</i> , the range is 1 to 4094.
mtu	(Optional) Displays a list of VLANs and the minimum and maximum transmission unit (MTU) sizes configured on ports in the VLAN.
name <i>vlan-name</i>	(Optional) Displays information about a single VLAN identified by the VLAN name. The VLAN name is an ASCII string from 1 to 32 characters.
remote-span	(Optional) Displays information about Remote SPAN (RSPAN) VLANs.
summary	(Optional) Displays VLAN summary information.



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

Command Default None

Command Modes User EXEC

	Release	Modification
Command History	Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines In the **show vlan mtu** command output, the MTU_Mismatch column shows whether all the ports in the VLAN have the same MTU. When yes appears in the column, it means that the VLAN has ports with different MTUs, and packets that are switched from a port with a larger MTU to a port with a smaller MTU might be dropped. If the VLAN does not have an SVI, the hyphen (-) symbol appears in the SVI_MTU column. If the MTU-Mismatch column displays yes, the names of the ports with the MinMTU and the MaxMTU appear.

This is an example of output from the **show vlan** command. See the table that follows for descriptions of the fields in the display.

```
Device> show vlan
VLAN Name                               Status      Ports
---- -----
1    default                             active     Gi1/0/2, Gi1/0/3, Gi1/0/4
                                         Gi1/0/5, Gi1/0/6, Gi1/0/7
                                         Gi1/0/8, Gi1/0/9, Gi1/0/10
                                         Gi1/0/11, Gi1/0/12, Gi1/0/13
                                         Gi1/0/14, Gi1/0/15, Gi1/0/16
                                         Gi1/0/17, Gi1/0/18, Gi1/0/19
                                         Gi1/0/20, Gi1/0/21, Gi1/0/22
                                         Gi1/0/23, Gi1/0/24, Gi1/0/25
                                         Gi1/0/26, Gi1/0/27, Gi1/0/28
                                         Gi1/0/29, Gi1/0/30, Gi1/0/31
                                         Gi1/0/32, Gi1/0/33, Gi1/0/34
                                         Gi1/0/35, Gi1/0/36, Gi1/0/37
                                         Gi1/0/38, Gi1/0/39, Gi1/0/40
                                         Gi1/0/41, Gi1/0/42, Gi1/0/43
                                         Gi1/0/44, Gi1/0/45, Gi1/0/46
```

```

Gi1/0/47, Gi1/0/48
2     VLAN0002          active
40    vlan=40            active
300   VLAN0300          active
1002  fddi-default      act/unsup
1003  token-ring-default act/unsup
1004  fddinet-default   act/unsup
1005  trnet-default     act/unsup

-----  

VLAN Type  SAID      MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2  

-----  

1   enet  100001  1500   -     -     -     -     -     0     0  

2   enet  100002  1500   -     -     -     -     -     0     0  

40  enet  100040  1500   -     -     -     -     -     0     0  

300 enet  100300  1500   -     -     -     -     -     0     0  

1002 fddi  101002  1500   -     -     -     -     -     0     0  

1003 tr   101003  1500   -     -     -     -     -     0     0  

1004 fdnet 101004  1500   -     -     -     ieee  -     0     0  

1005 trnet 101005  1500   -     -     -     ibm  -     0     0  

2000 enet  102000  1500   -     -     -     -     -     0     0  

3000 enet  103000  1500   -     -     -     -     -     0     0

-----  

Remote SPAN VLANs  

-----  

2000, 3000  

-----  

Primary Secondary Type          Ports  

-----  


```

Table 176: 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.

show vtp

Field	Description
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.
<i>interface-id</i>	(Optional) Interface for which to display VTP status and configuration. This can be a physical interface or a port channel.
password	Displays the configured VTP password (available in privileged EXEC mode only).

	status	Displays general information about the VTP management domain status.
Command Default	None	
Command Modes	User EXEC Privileged EXEC	
Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.
Usage Guidelines	When you enter the show vtp password command when the device is running VTP version 3, the display follows these rules:	
	<ul style="list-style-type: none"> If the password password global configuration command did not specify the hidden keyword and encryption is not enabled on the device, the password appears in clear text. If the password password command did not specify the hidden keyword and encryption is enabled on the device, the encrypted password appears. If the password password command included the hidden keyword, the hexadecimal secret key is displayed. 	
	This is an example of output from the show vtp devices command. A Yes in the Conflict column indicates that the responding server is in conflict with the local server for the feature; that is, when two devices in the same domain do not have the same primary server for a database.	
	<pre>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</pre>	
	This is an example of output from the show vtp counters command. The table that follows describes each field in the display.	
	<pre>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 -----</pre>	

show vtp

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 177: 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.
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.

Field	Description
Number of configuration revision errors	<p>Number of revision errors.</p> <p>Whenever you define a new VLAN, delete an existing one, suspend or resume an existing VLAN, or modify the parameters on an existing VLAN, the configuration revision number of the device increments.</p> <p>Revision errors increment whenever the device receives an advertisement whose revision number matches the revision number of the device, but the MD5 digest values do not match. This error means that the VTP password in the two devices is different or that the devices have different configurations.</p> <p>These errors indicate that the device is filtering incoming advertisements, which causes the VTP database to become unsynchronized across the network.</p>
Number of configuration digest errors	<p>Number of MD5 digest errors.</p> <p>Digest errors increment whenever the MD5 digest in the summary packet and the MD5 digest of the received advertisement calculated by the device do not match. This error usually means that the VTP password in the two devices is different. To solve this problem, make sure the VTP password on all devices is the same.</p> <p>These errors indicate that the device is filtering incoming advertisements, which causes the VTP database to become unsynchronized across the network.</p>
Number of V1 summary errors	<p>Number of Version 1 errors.</p> <p>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.</p>
Join Transmitted	Number of VTP pruning messages sent on the trunk.
Join Received	Number of VTP pruning messages received on the trunk.
Summary Advts Received from non-pruning-capable device	Number of VTP summary messages received on the trunk from devices that do not support pruning.

show vtp

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 LI1N0 (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 178: 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.
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.

Field	Description
VTP Operating Mode	<p>Displays the VTP operating mode, which can be server, client, or transparent.</p> <p>Server—A device in VTP server mode is enabled for VTP and sends advertisements. You can configure VLANs on it. The device guarantees that it can recover all the VLAN information in the current VTP database from NVRAM after reboot. By default, every device is a VTP server.</p> <p>Note The device automatically changes from VTP server mode to VTP client mode if it detects a failure while writing the configuration to NVRAM and cannot return to server mode until the NVRAM is functioning.</p>
	<p>Client—A device in VTP client mode is enabled for VTP, can send advertisements, but does not have enough nonvolatile storage to store VLAN configurations. You cannot configure VLANs on it. When a VTP client starts up, it does not send VTP advertisements until it receives advertisements to initialize its VLAN database.</p>
	<p>Transparent—A device in VTP transparent mode is disabled for VTP, does not send or learn from advertisements sent by other devices, and cannot affect VLAN configurations on other devices in the network. The device receives VTP advertisements and forwards them on all trunk ports except the one on which the advertisement was received.</p>
Maximum VLANs Supported Locally	Maximum number of VLANs supported locally.
Number of Existing VLANs	Number of existing VLANs.
Configuration Revision	Current configuration revision number on this device.
MD5 Digest	A 16-byte checksum of the VTP configuration.

This is an example of output from the **show vtp status** command for a device running VTP version 3:

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 trunk

```
switchport priority extend {cos value | trust}
no switchport priority extend
```

Syntax Description	cos value Sets the IP phone port to override the IEEE 802.1p priority received from the PC or the attached device with the specified class of service (CoS) value. The range is 0 to 7. Seven is the highest priority. The default is 0.				
	trust Sets the IP phone port to trust the IEEE 802.1p priority received from the PC or the attached device.				
Command Default	The default port priority is set to a CoS value of 0 for untagged frames received on the port.				
Command Modes	Interface configuration				
Command History	<table border="1"> <thead> <tr> <th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td><td>This command was introduced.</td></tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.6.1	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.6.1	This command was introduced.				

Usage Guidelines	When voice VLAN is enabled, you can configure the device to send the Cisco Discovery Protocol (CDP) packets to instruct the IP phone how to send data packets from the device attached to the access port on the Cisco IP Phone. You must enable CDP on the device port connected to the Cisco IP Phone to send the configuration to the Cisco IP Phone. (CDP is enabled by default globally and on all device interfaces.) You should configure voice VLAN on device access ports.
-------------------------	--

This example shows how to configure the IP phone connected to the specified port to trust the received IEEE 802.1p priority:

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# switchport priority extend trust
```

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

switchport trunk

To set the trunk characteristics when the interface is in trunking mode, use the **switchport trunk** command in interface configuration mode. To reset a trunking characteristic to the default, use the **no** form of this command.

```
switchport trunk {allowed vlan vlan-list | native vlan vlan-id | pruning vlan vlan-list}
no switchport trunk {allowed vlan | native vlan | pruning vlan}
```

Syntax Description	allowed vlan vlan-list Sets the list of allowed VLANs that can receive and send traffic on this interface in tagged format when in trunking mode. See the Usage Guidelines for the <i>vlan-list</i> 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 Everest 16.6.1	This command was introduced.
--------------------------------	------------------------------

Usage Guidelines

The *vlan-list* format is **all | none | [add | remove | except] *vlan-atom* [,*vlan-atom...*]**:

- **all** specifies all VLANs from 1 to 4094. This is the default. This keyword is not allowed on commands that do not permit all VLANs in the list to be set at the same time.
- **none** specifies an empty list. This keyword is not allowed on commands that require certain VLANs to be set or at least one VLAN to be set.
- **add** adds the defined list of VLANs to those currently set instead of replacing the list. Valid IDs are from 1 to 1005; extended-range VLANs (VLAN IDs greater than 1005) are valid in some cases.



Note You can add extended-range VLANs to the allowed VLAN list, but not to the pruning-eligible VLAN list.

Separate nonconsecutive VLAN IDs with a comma; use a hyphen to designate a range of IDs.

- **remove** removes the defined list of VLANs from those currently set instead of replacing the list. Valid IDs are from 1 to 1005; extended-range VLAN IDs are valid in some cases.



Note You can remove extended-range VLANs from the allowed VLAN list, but you cannot remove them from the pruning-eligible list.

- **except** lists the VLANs that should be calculated by inverting the defined list of VLANs. (VLANs are added except the ones specified.) Valid IDs are from 1 to 1005. Separate nonconsecutive VLAN IDs with a comma; use a hyphen to designate a range of IDs.
- *vlan-atom* is either a single VLAN number from 1 to 4094 or a continuous range of VLANs described by two VLAN numbers, the lesser one first, separated by a hyphen.

Native VLANs:

- All untagged traffic received on an IEEE 802.1Q trunk port is forwarded with the native VLAN configured for the port.
- If a packet has a VLAN ID that is the same as the sending-port native VLAN ID, the packet is sent without a tag; otherwise, the switch sends the packet with a tag.
- The **no** form of the **native vlan** command resets the native mode VLAN to the appropriate default VLAN for the device.

Allowed VLAN:

- To reduce the risk of spanning-tree loops or storms, you can disable VLAN 1 on any individual VLAN trunk port by removing VLAN 1 from the allowed list. When you remove VLAN 1 from a trunk port, the interface continues to send and receive management traffic, for example, Cisco Discovery Protocol (CDP), Port Aggregation Protocol (PAgP), Link Aggregation Control Protocol (LACP), Dynamic Trunking Protocol (DTP), and VLAN Trunking Protocol (VTP) in VLAN 1.
- The **no** form of the **allowed vlan** command resets the list to the default list, which allows all VLANs.

Trunk pruning:

- The pruning-eligible list applies only to trunk ports.
- Each trunk port has its own eligibility list.
- If you do not want a VLAN to be pruned, remove it from the pruning-eligible list. VLANs that are pruning-ineligible receive flooded traffic.
- VLAN 1, VLANs 1002 to 1005, and extended-range VLANs (VLANs 1006 to 4094) cannot be pruned.

This example shows how to configure VLAN 3 as the default for the port to send all untagged traffic:

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# switchport trunk native vlan 3
```

This example shows how to add VLANs 1, 2, 5, and 6 to the allowed list:

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# switchport trunk allowed vlan add 1,2,5,6
```

This example shows how to remove VLANs 3 and 10 to 15 from the pruning-eligible list:

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# switchport trunk pruning vlan remove 3,10-15
```

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

vlan

To add a VLAN and to enter the VLAN configuration mode, use the **vlan** command in global configuration mode. To delete the VLAN, use the **no** form of this command.

vlan *vlan-id*

no vlan *vlan-id*

Syntax Description	<i>vlan-id</i> ID of the VLAN to be added and configured. The range is 1 to 4094. You can enter a single VLAN ID, a series of VLAN IDs separated by commas, or a range of VLAN IDs separated by hyphens.
---------------------------	--

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

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

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines	You can use the vlan <i>vlan-id</i> global configuration command to add normal-range VLANs (VLAN IDs 1 to 1005) or extended-range VLANs (VLAN IDs 1006 to 4094). Configuration information for normal-range VLANs is always saved in the VLAN database, and you can display this information by entering the show vlan privileged EXEC command. If the VTP mode is transparent, VLAN configuration information for normal-range VLANs is also saved in the device running configuration file. VLAN IDs in the extended range are not saved in the VLAN database, but they are stored in the switch running configuration file, and you can save the configuration in the startup configuration file.
-------------------------	--

VTP version 3 supports propagation of extended-range VLANs. VTP versions 1 and 2 propagate only VLANs 1 to 1005.

When you save the VLAN and VTP configurations in the startup configuration file and reboot the device, the configuration is selected as follows:

- If the VTP mode is transparent in the startup configuration and the VLAN database and the VTP domain name from the VLAN database matches that in the startup configuration file, the VLAN database is ignored (cleared), and the VTP and VLAN configurations in the startup configuration file are used. The VLAN database revision number remains unchanged in the VLAN database.
- If the VTP mode or domain name in the startup configuration do not match the VLAN database, the domain name and VTP mode and configuration for VLAN IDs 1 to 1005 use the VLAN database information.

If you enter an invalid VLAN ID, you receive an error message and do not enter VLAN configuration mode.

Entering the **vlan** command with a VLAN ID enables VLAN configuration mode. When you enter the VLAN ID of an existing VLAN, you do not create a new VLAN, but you can modify VLAN parameters for that VLAN. The specified VLANs are added or modified when you exit the VLAN configuration mode. Only the **shutdown** command (for VLANs 1 to 1005) takes effect immediately.



Note	Although all commands are visible, the only VLAN configuration command that is supported on extended-range VLANs is remote-span . For extended-range VLANs, all other characteristics must remain at the default state.
-------------	--

These configuration commands are available in VLAN configuration mode. The **no** form of each command returns the characteristic to its default state:

- **are *are-number***—Defines the maximum number of all-routes explorer (ARE) hops for this VLAN. This keyword applies only to TrCRF VLANs. The range is 0 to 13. The default is 7. If no value is entered, 0 is assumed to be the maximum.
- **backupcrf**—Specifies the backup CRF mode. This keyword applies only to TrCRF VLANs.
 - **enable**—Backup CRF mode for this VLAN.
 - **disable**—Backup CRF mode for this VLAN (the default).
- **bridge {bridge-number | type}**—Specifies the logical distributed source-routing bridge, the bridge that interconnects all logical rings that have this VLAN as a parent VLAN in FDDI-NET, Token Ring-NET, and TrBRF VLANs. The range is 0 to 15. The default bridge number is 0 (no source-routing bridge) for FDDI-NET, TrBRF, and Token Ring-NET VLANs. The **type** keyword applies only to TrCRF VLANs and is one of these:
 - **srb**—Source-route bridging
 - **srt**—Source-route transparent) bridging VLAN
- **exit**—Applies changes, increments the VLAN database revision number (VLANs 1 to 1005 only), and exits VLAN configuration mode.
- **media**—Defines the VLAN media type and is one of these:



Note The device supports only Ethernet ports. You configure only FDDI and Token Ring media-specific characteristics for VLAN Trunking Protocol (VTP) global advertisements to other devices. These VLANs are locally suspended.

- **ethernet**—Ethernet media type (the default).
- **fd-net**—FDDI network entity title (NET) media type.
- **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 179: Valid Commands and Syntax for Different Media Types

Media Type	Valid Syntax
Ethernet	name vlan-name, media ethernet, state {suspend active}, said said-value, remote-span, tb-vlan1 tb-vlan1-id, tb-vlan2 tb-vlan2-id
FDDI	name vlan-name, media fddi, state {suspend active}, said said-value, ring ring-number, parent parent-vlan-id, tb-vlan1 tb-vlan1-id, tb-vlan2 tb-vlan2-id

Media Type	Valid Syntax
FDDI-NET	name <i>vlan-name</i> , media fd-net , state {suspend active}, said <i>said-value</i> , bridge <i>bridge-number</i> , stp type {ieee ibm auto}, tb-vlan1 <i>tb-vlan1-id</i> , tb-vlan2 <i>tb-vlan2-id</i> If VTP v2 mode is disabled, do not set the stp type to auto .
Token Ring	VTP v1 mode is enabled. name <i>vlan-name</i> , media tokenring, state {suspend active}, said <i>said-value</i> , ring <i>ring-number</i> , parent parent-vlan-id , tb-vlan1 <i>tb-vlan1-id</i> , tb-vlan2 tb-vlan2-id
Token Ring concentrator relay function (TrCRF)	VTP v2 mode is enabled. name <i>vlan-name</i> , media tokenring, state {suspend active}, said <i>said-value</i> , ring <i>ring-number</i> , parent parent-vlan-id , bridge type {srp srt}, are are-number , ste ste-number , backuperf {enable disable}, tb-vlan1 <i>tb-vlan1-id</i> , tb-vlan2 <i>tb-vlan2-id</i>
Token Ring-NET	VTP v1 mode is enabled. name <i>vlan-name</i> , media tr-net, state {suspend active}, said <i>said-value</i> , bridge <i>bridge-number</i> , stp type {ieee ibm}, tb-vlan1 <i>tb-vlan1-id</i> , tb-vlan2 tb-vlan2-id
Token Ring bridge relay function (TrBRF)	VTP v2 mode is enabled. name <i>vlan-name</i> , media tr-net, state {suspend active}, said <i>said-value</i> , bridge <i>bridge-number</i> , stp type {ieee ibm auto}, tb-vlan1 <i>tb-vlan1-id</i> , tb-vlan2 tb-vlan2-id

The following table describes the rules for configuring VLANs:

Table 180: 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.

Configuration	Rule
VTP v2 mode is enabled, and you are configuring a TrBRF VLAN media type.	Specify a bridge number. Do not leave this field blank.
VTP v1 mode is enabled.	No VLAN can have an STP type set to auto. This rule applies to Ethernet, FDDI, FDDI-NET, Token Ring, and Token Ring-NET VLANs.
Add a VLAN that requires translational bridging (values are not set to zero).	The translational bridging VLAN IDs that are used must already exist in the database. The translational bridging VLAN IDs that a configuration points to must also contain a pointer to the original VLAN in one of the translational bridging parameters (for example, Ethernet points to FDDI, and FDDI points to Ethernet). The translational bridging VLAN IDs that a configuration points to must be different media types than the original VLAN (for example, Ethernet can point to Token Ring). If both translational bridging VLAN IDs are configured, these VLANs must be different media types (for example, Ethernet can point to FDDI and Token Ring).

This example shows how to add an Ethernet VLAN with default media characteristics. The default includes a *vlan-name* of VLAN xxxx, where xxxx represents four numeric digits (including leading zeros) equal to the VLAN ID number. The default media is ethernet; the state is active. The default said-value is 100000 plus the VLAN ID; the mtu-size variable is 1500; the stp-type is ieee. When you enter the **exit** VLAN configuration command, the VLAN is added if it did not already exist; otherwise, this command does nothing.

This example shows how to create a new VLAN with all default characteristics and enter VLAN configuration mode:

```
Device(config)# vlan 200
Device(config-vlan)# exit
Device(config)#
```

This example shows how to create a new extended-range VLAN with all the default characteristics, to enter VLAN configuration mode, and to save the new VLAN in the device startup configuration file:

```
Device(config)# vlan 2000
Device(config-vlan)# end
Device# copy running-config startup config
```

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

vtp (global configuration)

To set or modify the VLAN Trunking Protocol (VTP) configuration characteristics, use the **vtp** command in global configuration mode. To remove the settings or to return to the default settings, use the **no** form of this command.

```
vtp {domain domain-name | file filename | interface interface-name [only] | mode {client | off | server | transparent} [{mst | unknown | vlan}] | password password [{hidden | secret}] | pruning | version number}
no vtp {file | interface | mode [{client | off | server | transparent}] [{mst | unknown | vlan}] | password | pruning | version}
```

Syntax Description	
domain <i>domain-name</i>	Specifies the VTP domain name, an ASCII string from 1 to 32 characters that identifies the VTP administrative domain for the device. The domain name is case sensitive.
file <i>filename</i>	Specifies the Cisco IOS file system file where the VTP VLAN configuration is stored.
interface <i>interface-name</i>	Specifies the name of the interface providing the VTP ID updated for this device.
only	(Optional) Uses only the IP address of this interface as the VTP IP updater.
mode	Specifies the VTP device mode as client, server, or transparent.
client	Places the device in VTP client mode. A device in VTP client mode is enabled for VTP, and can send advertisements, but does not have enough nonvolatile storage to store VLAN configurations. You cannot configure VLANs on a VTP client. VLANs are configured on another device in the domain that is in server mode. When a VTP client starts up, it does not send VTP advertisements until it receives advertisements to initialize its VLAN database.
off	Places the device in VTP off mode. A device in VTP off mode functions the same as a VTP transparent device except that it does not forward VTP advertisements on trunk ports.
server	Places the device in VTP server mode. A device in VTP server mode is enabled for VTP and sends advertisements. You can configure VLANs on the device. The device can recover all the VLAN information in the current VTP database from nonvolatile storage after reboot.
transparent	Places the device in VTP transparent mode. A device in VTP transparent mode is disabled for VTP, does not send advertisements or learn from advertisements sent by other devices, and cannot affect VLAN configurations on other devices in the network. The device receives VTP advertisements and forwards them on all trunk ports except the one on which the advertisement was received. When VTP mode is transparent, the mode and domain name are saved in the device running configuration file, and you can save them in the device startup configuration file by entering the copy running-config startup config privileged EXEC command.
mst	(Optional) Sets the mode for the multiple spanning tree (MST) VTP database (only VTP Version 3).

unknown	(Optional) Sets the mode for unknown VTP databases (only VTP Version 3).
vlan	(Optional) Sets the mode for VLAN VTP databases. This is the default (only VTP Version 3).
password <i>password</i>	Sets the administrative domain password for the generation of the 16-byte secret value used in MD5 digest calculation to be sent in VTP advertisements and to validate received VTP advertisements. The password can be an ASCII string from 1 to 32 characters. The password is case sensitive.
hidden	(Optional) Specifies that the key generated from the password string is saved in the VLAN database file. When the hidden keyword is not specified, the password string is saved in clear text. When the hidden password is entered, you need to reenter the password to issue a command in the domain. This keyword is supported only in VTP Version 3.
secret	(Optional) Allows the user to directly configure the password secret key (only VTP Version 3).
pruning	Enables VTP pruning on the device.
version <i>number</i>	Sets the VTP Version to Version 1, Version 2, or Version 3.

Command Default

The default filename is *flash:vlan.dat*.

The default mode is server mode and the default database is VLAN.

In VTP Version 3, for the MST database, the default mode is transparent.

No domain name or password is defined.

No password is configured.

Pruning is disabled.

The default version is Version 1.

Command Modes

Global configuration

Command History**Release** **Modification**

Cisco IOS XE Everest 16.6.1 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.

vtp (global configuration)

The **vtp file** *filename* cannot be used to load a new database; it renames only the file in which the existing database is stored.

Follow these guidelines when configuring a VTP domain name:

- The device is in the no-management-domain state until you configure a domain name. While in the no-management-domain state, the device does not send any VTP advertisements even if changes occur to the local VLAN configuration. The device leaves the no-management-domain state after it receives the first VTP summary packet on any port that is trunking or after you configure a domain name by using the **vtp domain** command. If the device receives its domain from a summary packet, it resets its configuration revision number to 0. After the device leaves the no-management-domain state, it cannot be configured to reenter it until you clear the NVRAM and reload the software.
- Domain names are case-sensitive.
- After you configure a domain name, it cannot be removed. You can only reassign it to a different domain.

Follow these guidelines when setting VTP mode:

- The **no vtp mode** command returns the device to VTP server mode.
- The **vtp mode server** command is the same as **no vtp mode** except that it does not return an error if the device is not in client or transparent mode.
- If the receiving device is in client mode, the client device changes its configuration to duplicate the configuration of the server. If you have devices in client mode, be sure to make all VTP or VLAN configuration changes on a device in server mode, as it has a higher VTP configuration revision number. If the receiving device is in transparent mode, the device configuration is not changed.
- A device in transparent mode does not participate in VTP. If you make VTP or VLAN configuration changes on a device in transparent mode, the changes are not propagated to other devices in the network.
- If you change the VTP or VLAN configuration on a device that is in server mode, that change is propagated to all the devices in the same VTP domain.
- The **vtp mode transparent** command disables VTP from the domain but does not remove the domain from the device.
- In VTP Versions 1 and 2, the VTP mode must be transparent for VTP and VLAN information to be saved in the running configuration file.
- With VTP Versions 1 and 2, you cannot change the VTP mode to client or server if extended-range VLANs are configured on the switch. Changing the VTP mode is allowed with extended VLANs in VTP Version 3.
- The VTP mode must be transparent for you to add extended-range VLANs or for VTP and VLAN information to be saved in the running configuration file.
- VTP can be set to either server or client mode only when dynamic VLAN creation is disabled.
- The **vtp mode off** command sets the device to off. The **no vtp mode off** command resets the device to the VTP server mode.

Follow these guidelines when setting a VTP password:

- Passwords are case sensitive. Passwords should match on all devices in the same domain.
- When you use the **no vtp password** form of the command, the device returns to the no-password state.

- The **hidden** and **secret** keywords are supported only in VTP Version 3. If you convert from VTP Version 2 to VTP Version 3, you must remove the hidden or secret keyword before the conversion.

Follow these guidelines when setting VTP pruning:

- VTP pruning removes information about each pruning-eligible VLAN from VTP updates if there are no stations belonging to that VLAN.
- If you enable pruning on the VTP server, it is enabled for the entire management domain for VLAN IDs 1 to 1005.
- Only VLANs in the pruning-eligible list can be pruned.
- Pruning is supported with VTP Version 1 and Version 2.

Follow these guidelines when setting the VTP version:

- Toggling the Version 2 (v2) mode state modifies parameters of certain default VLANs.
- Each VTP device automatically detects the capabilities of all the other VTP devices. To use Version 2, all VTP devices in the network must support Version 2; otherwise, you must configure them to operate in VTP Version 1 mode.
- If all devices in a domain are VTP Version 2-capable, you only need to configure Version 2 on one device; the version number is then propagated to the other Version-2 capable devices in the VTP domain.
- If you are using VTP in a Token Ring environment, VTP Version 2 must be enabled.
- If you are configuring a Token Ring bridge relay function (TrBRF) or Token Ring concentrator relay function (TrCRF) VLAN media type, you must use Version 2.
- If you are configuring a Token Ring or Token Ring-NET VLAN media type, you must use Version 1.
- In VTP Version 3, all database VTP information is propagated across the VTP domain, not only VLAN database information.
- Two VTP Version 3 regions can only communicate over a VTP Version 1 or VTP Version 2 region in transparent mode.

You cannot save password, pruning, and version configurations in the device configuration file.

This example shows how to rename the filename for VTP configuration storage to vtpfilename:

```
Device(config)# vtp file vtpfilename
```

This example shows how to clear the device storage filename:

```
Device(config)# no vtp file vtpconfig  
Clearing device storage filename.
```

This example shows how to specify the name of the interface providing the VTP updater ID for this device:

```
Device(config)# vtp interface gigabitethernet
```

This example shows how to set the administrative domain for the device:

vtp (interface configuration)

```
Device(config)# vtp domain OurDomainName
```

This example shows how to place the device in VTP transparent mode:

```
Device(config)# vtp mode transparent
```

This example shows how to configure the VTP domain password:

```
Device(config)# vtp password ThisIsOurDomainsPassword
```

This example shows how to enable pruning in the VLAN database:

```
Device(config)# vtp pruning
Pruning switched ON
```

This example shows how to enable Version 2 mode in the VLAN database:

```
Device(config)# vtp version 2
```

You can verify your settings by entering the **show vtp status** privileged EXEC command.

vtp (interface configuration)

To enable the VLAN Trunking Protocol (VTP) on a per-port basis, use the **vtp** command in interface configuration mode. To disable VTP on the interface, use the **no** form of this command.

```
vtp
no vtp
```

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Interface configuration

Command History	Release	Modification
Cisco IOS XE Everest 16.6.1	Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines Enter this command only on interfaces that are in trunking mode.

This example shows how to enable VTP on an interface:

```
Device(config-if)# vtp
```

This example shows how to disable VTP on an interface:

```
Device(config-if)# no vtp
```

vtp primary

To configure a device as the VLAN Trunking Protocol (VTP) primary server, use the **vtp primary** command in privileged EXEC mode.

vtp primary [{mst | vlan}] [force]

Syntax Description	mst (Optional) Configures the device as the primary VTP server for the multiple spanning tree (MST) feature. vlan (Optional) Configures the device as the primary VTP server for VLANs. force (Optional) Configures the device to not check for conflicting devices when configuring the primary server.
---------------------------	---

Command Default The device is a VTP secondary server.

Command Modes Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines A VTP primary server updates the database information and sends updates that are honored by all devices in the system. A VTP secondary server can only back up the updated VTP configurations received from the primary server to NVRAM.

By default, all devices come up as secondary servers. Primary server status is needed only for database updates when the administrator issues a takeover message in the domain. You can have a working VTP domain without any primary servers.

Primary server status is lost if the device reloads or domain parameters change.



Note This command is supported only when the device is running VTP Version 3.

This example shows how to configure the device as the primary VTP server for VLANs:

```
Device# vtp primary vlan
Setting device to VTP TRANSPARENT mode.
```

You can verify your settings by entering the **show vtp status** privileged EXEC command.

vtp primary

Notices

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

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

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

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

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

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

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.

