

Cisco IOS XE Catalyst SD-WAN Qualified Command Reference Guide

First Published: 2021-01-29

Last Modified: 2026-10-19

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

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

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

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

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

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

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

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

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

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

© 2021–2026 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1 **Read Me First** 1

CHAPTER 2 **What's New in Cisco IOS XE (Catalyst SD-WAN)** 3

CHAPTER 3 **Introduction** 5

CHAPTER 4 **AAA Commands** 7

- aaa accounting 7
- aaa authentication attempts login 10
- aaa authentication enable default 10
- aaa authentication login 11
- aaa authentication password-prompt 13
- aaa authentication ppp 13
- aaa authentication username-prompt 14
- aaa authorization 15
- aaa authorization config-commands 16
- aaa authorization console 17
- aaa authorization credential download default 18
- aaa lockout-policy 19
- aaa group server tacacs+ 20
- aaa netconf-accounting 20
- ip tacacs source-interface 21
- ip vrf forwarding (server-group) 22
- lockout-policy 23
- login block-for 25
- login quiet-mode access-class 26

login-rate 27
multi-factor-auth duo 27
server-private (TACACS+) 29
tacacs server address ipv4 30
tacacs server key 31
tacacs server port 31
tacacs server timeout 32

CHAPTER 5 ACL Commands 35
deny 35
ip access-list 38
ipv6 access-list 39
permit 39
sequence 42

CHAPTER 6 AppNav Commands 43
appnav-controller 43
service-insertion 44
service-insertion appnav-controller-group 45
service-node-group 46
service-insertion waas interface 47
service node 47
service-policy 48

CHAPTER 7 AppQoE Commands 49
(config-scxt) appnav-controller-group 49
app-resource package-profile 50
appqoe http-connect 51
appqoe tcpopt enable 51
app-hosting 52
app-hosting appid 53
app-vnic 54
cluster-type 55
device-role 55

dreopt enable 56
dual-side optimization enable 56
exporter 57
guest-ipaddress 58
iox 59
performance monitor apply 59
performance monitor context 60
performance monitor sampling-rate 61
platform resource 62
rd 63
sdwan appqoe dreopt enable 63
service-insertion appqoe 64
service-insertion appnav-controller-group appqoe 64
service-insertion service-node-group appqoe 66
start (app-hosting) 66
traffic-monitor 67
vrf (service-insertion-context) 68

CHAPTER 8 ATM-native Commands 71
encapsulation (ATM) 71
interface ATM 73
oam-pvc 74
oam retry 75
pvc 76
service-policy 77
vbr-nrt 78
Physical and Logical ATM Interface Commands 79
bridge-dot1q encap 79
dialer pool-member 79
ip mtu 80
load-interval 81
protocol (ATM) 82

CHAPTER 9 BFD Commands 85

alarms alarm bfd-state-change syslog 85
bfd app-route 86
bfd enhanced-app-route 87
bfd color 88
hello-interval 89
pmtu-discovery 89

CHAPTER 10 BGP Commands 91
address-family ipv4 (BGP) 92
address-family ipv6 93
aggregate-address 93
bandwidth (policy-map class) 94
bgp always-compare-med 95
bgp bestpath as-path multipath-relax 96
bgp bestpath compare-routerid 97
bgp bestpath med missing-as-worst 98
bgp deterministic-med 98
bgp graceful-restart 99
bgp log-neighbor-changes 99
bandwidth remaining ratio 100
class (policy-map) 101
distance bgp 102
exit-address-family (bgp) 103
maximum-paths eibgp 104
neighbor advertise-map 104
neighbor advertisement-interval 105
neighbor description 106
neighbor ebgp-multihop 107
neighbor ha-mode graceful-restart 108
neighbor maximum-prefix (BGP) 108
neighbor next-hop-self 109
neighbor password 110
neighbor remote-as 111
neighbor route-map 112

neighbor send-community 113
neighbor shutdown 113
neighbor timers 114
network (BGP and multiprotocol BGP) 115
police (percent) 115
policy-map 116
priority level 117
redistribute (IP) 118
redistribute omp (bgp) 120
router bgp 121
timers bgp 122

CHAPTER 11 Cellular Commands 123
lte gps (cellular) 123
lte sim 125
profile id 125
lte gps constellation 127
lte modem crash-action 127
lte profile reset 128
lte modem dm-log 129
lte450 profile 130
lte450 credential 132
lte450 band 133

CHAPTER 12 CFM Commands 135
alarm 135
cfm mep domain 136
cos 137
ethernet cfm ieee 137
ethernet cfm global 137
ethernet oam 138
ethernet oam remote-loopback 138
ethernet loopback permit 139
snmp-server enable traps ethernet cfm cc 139

snmp-server enable traps ethernet cfm crosscheck 140
ethernet evc 140
ethernet cfm domain level 140
offload sampling 141
sender-id 142
service (CFM-srv) 143
service evc 144
continuity-check 144

CHAPTER 13 Cisco Survivable Remote Site Telephony Commands 147
Cisco Survivable Remote Site Telephony Commands 147
SRST Commands 147

CHAPTER 14 Cisco TrustSec 149
aaa authorization network 150
aaa group server radius 150
aaa server radius dynamic-author 151
accept-lifetime 151
client 152
cryptographic-algorithm 152
cts authorization list network 153
cts credentials 154
cts role-based enforcement 154
cts role-based permissions 155
cts role-based sgt-map 156
cts sgt 156
cts sxp connection peer 157
cts sxp default key-chain 158
cts sxp default password 159
cts sxp default source-ip 160
cts sxp enable 160
cts sxp listener hold-time 161
cts sxp log binding-changes 161
cts manual 162

cts sxp node-id 162
cts sxp reconciliation period 163
cts sxp retry period 163
cts sxp speaker hold-time 164
domain stripping 164
ip radius source-interface 165
ip vrf forwarding 165
key 165
key chain 166
key-string 166
port 167
recv-id 167
send-id 168
send-lifetime 169
server-private (RADIUS) 169

CHAPTER 15 Cisco Unified Border Element Commands 171
CUBE Commands 172

CHAPTER 16 Class-Map Commands 181
class-map 181
match qos-group 183
pass 184

CHAPTER 17 Cloud OnRamp for SaaS Commands 187
probe-path load-balance-dia latency-variance 187
probe-path load-balance-dia loss-variance 189
probe-path load-balance-dia source-ip-hash 191
probe saas-app 192
probe saas-app webex 193

CHAPTER 18 Crypto Commands 195
aaa authorization (IKEv2 profile) 196
address (IKEv2 keyring) 197

authentication (IKEv2 profile) 198
config-exchange 199
crypto ikev2 authorization policy 200
crypto ikev2 diagnose 200
crypto ikev2 keyring 201
crypto ikev2 limit 202
crypto ikev2 policy 203
crypto ikev2 profile 203
crypto ikev2 proposal 204
crypto ipsec profile 205
crypto ipsec transform-set 206
crypto isakmp aggressive-mode disable 207
crypto pki import 207
crypto pki trustpoint 208
encryption (IKEv2 proposal) 209
enrollment selfsigned 210
group (IKEv2 proposal) 210
integrity 211
keyring (IKEv2 profile) 211
lifetime (IKEv2 profile) 212
match identity remote 213
mode (IPSec) 214
multi-tenancy 215
parameter-map type inspect-global 216
peer 217
pre-shared-key 218
proposal 219
revocation-check 220
set ikev2-profile 220
set pfs 221
set security-association lifetime 223
set security-association replay window-size 224
set transform-set 224
subject-name 225

CHAPTER 19 EIGRP Commands 227

address-family ipv4 vrf autonomous-system 227

af-interface 228

dampening-change 229

dampening-interval 230

exit-address-family 230

exit-af-interface 231

exit-af-topology 232

hello-interval 233

hold-time 233

neighbor (EIGRP) 234

network (EIGRP) 235

redistribute omp metric 236

redistribute static 237

router eigrp 237

split-horizon (EIGRP) 238

topology (EIGRP) 239

CHAPTER 20 Event Commands 241

action (EEM) 241

event ipsla 244

event manager applet 246

event manager session cli username 247

event none 247

event routing 248

event syslog 250

event timer 251

event track 253

CHAPTER 21 Frame-Relay-Native Commands 255

frame-relay lmi-type 255

frame-relay intf-type 256

frame-relay interface-dlci 257

frame-relay multilink bandwidth-class 258
interface 259
interface MFR 262
ip address 263
encapsulation frame-relay 264

CHAPTER 22 **Global Configuration Commands** 265
clock 265
config-transaction 266
crypto isakmp diagnose error 267
hostname 268
line 268
login authentication 269
login on-success log 270
mac address-table aging-time 271
mac address-table static 272
memory free low-watermark processor 272
platform qfp utilization monitor load 273
platform-resource 274
sdwan 274
service password-recovery 275
service tcp-small-servers 275
service timestamps 276
service udp-small-servers 278
speed 279
speedtest disable-backward-compatible-ip 279
stopbits 280
transport input 281
transport output 281
username 282

CHAPTER 23 **high-availability** 285
redundancy 285
application redundancy 286

preempt 286
init-role 287
path-optimization 287
redundancy rii 288

CHAPTER 24 Hub and Spoke 289
topology hub-and-spoke enable 289

CHAPTER 25 HSRP Commands 291
standby authentication 291
standby follow 293
standby ip 293
standby ipv6 294
standby mac-address 295
standby mac-refresh 296
standby name 296
standby preempt 297
standby priority 298
standby timers 299
standby track 300
standby version 302

CHAPTER 26 Ignition Power Management Commands 303
ignition enable 303
ignition sense 304
ignition battery-type 305
ignition off-timer 305
ignition undervoltage threshold 306
ignition sense-voltage threshold 307
ignition sense-voltage on-threshold off-threshold 307

CHAPTER 27 Interface Commands 309
address (VRRP) 310
channel-group 311

border 311
description (interface configuration) 312
duplex 313
encapsulation 313
hold-queue 314
hw-module subslot breakout 315
interface 316
interface-pair 320
interface vlan 322
ip address 323
ip address dhcp 324
ip policy route-map 324
lacp port-priority 325
lacp system-priority 326
load-balancing 327
mtu 327
negotiation 328
Port-channel 328
port-channel load-balance 329
port-channel load-balance-hash-algo 330
port-settings 331
preempt (VRRP) 332
priority vrrp 333
shutdown (controller) 334
speed 334
switchport access vlan 336
switchport mode 336
timers advertise VRRP 337
tunnel destination 338
tunnel mode 339
tunnel route-via 340
tunnel source 340
track ip route 341
track 342

track (VRRP) 343
vrf forwarding 344
vrrp address-family 345
vrrpv2 346

CHAPTER 28 IP Commands 347
access-class 349
address prefix 350
arp timeout 350
cdp enable 351
cdp run 351
default-router 352
dns-server 352
domain-name 353
ip address 354
ip address dhcp 355
ip arp proxy disable 355
ip bootp server 356
ip cef load-sharing algorithm 357
ip-clear-dont-fragment 358
ip community-list 359
ip dhcp client vendor-class 361
ip dhcp conflict logging 362
ip dhcp use 363
ip dhcp smart-relay 364
ip dhcp use hardware-address client-id 365
ip directed-broadcast 365
ip dns server 366
ip domain lookup 367
ip finger 367
ip helper-address 368
ip host 368
ip host ip-address 369
ip http authentication 370

ip http client source-interface 371
ip http secure-server 371
ip http server 372
ip http tls-version 373
ip icmp rate-limit unreachable 373
ip icmp redirect 374
ip igmp ssm-map query dns 375
ip load-sharing algorithm 375
ip mtu 376
ip multicast route-limit 377
ip name-server 378
ip pim 379
ip pim bsr-candidate 379
ip pim rp-address 381
ip pim rp-candidate 381
ip prefix-list 383
ip redirects 383
ip rcmd 384
ip rcmd rcp-enable 385
ip rcmd rsh-enable 386
ip route vrf 386
ip route 387
ip source-route 388
ip ssh version 389
ip tcp adjust-mss 390
ip tcp mss 390
ip unnumbered 391
ip virtual-reassembly 391
ipv6 access-class 392
ipv6 address 393
ipv6 address autoconfig 394
ipv6 address dhcp client request 394
ipv6 cef load-sharing algorithm 394
ipv6 dhcp client pd 396

ipv6 dhcp client vendor-class 396
ipv6 dhcp pool 397
ipv6 dhcp relay destination 398
ipv6 dhcp-relay option vpn 398
ipv6 dhcp server 399
ipv6 enable 399
ipv6 load-sharing algorithm 400
ipv6 nd other-config-flag 401
ipv6 nd prefix 401
ipv6 nd ra suppress 402
ipv6 nd router-preference 403
ipv6 redirects 404
ipv6 route 404
ipv6-strict-control 405
ipv6 unnumbered 406
lease 407
network (DHCP) 407
option (DHCP) 408
prefix-delegation 409
prefix-delegation pool 409
spt-only 409
vlan internal allocation policy 410
vendor-specific 411
vrf (DHCP pool) 411

CHAPTER 29 **IP Routing: OSPF Commands** 413

ip ospf area 413
ip ospf authentication 414
ip ospf cost 414
ip ospf dead-interval 415
ip ospf hello-interval 415
ip ospf message-digest-key md5 416
ip ospf network 417
ip ospf priority 417

ip ospf retransmit-interval 418

CHAPTER 30 L2VPN Commands 419

l2vpn sdwan instance 419

bridge-domain 420

l2protocol peer 422

l2protocol forward 423

CHAPTER 31 LAN Switching Commands 427

spanning-tree bpduguard 427

spanning-tree guard 427

spanning-tree mode 428

spanning-tree portfast (interface) 428

CHAPTER 32 Line Commands 431

exec-timeout 431

ip telnet disable 432

line 433

line con transport 434

line vty transport 435

line aux transport 437

password (line configuration) 438

privilege level 439

CHAPTER 33 Logging Commands 441

banner login 441

logging buffered 442

logging console 443

logging discriminator 443

logging host 445

logging monitor 446

logging persistent 446

logging rate-limit 447

logging source-interface 448

logging tls-profile ciphersuite 448
logging tls-profile tls-version 450
logging trap 450
logging trap informational syslog-format rfc5424 451
service timestamps 452

CHAPTER 34 MACsec Commands 455
key chain 455
key 456
key-string 457
cryptographic-algorithm 458
lifetime 459
mka policy 460
confidentiality-offset 461
delay-protection 461
include-icv-indicator 462
key-server 462
macsec-cipher-suite 463
sak-rekey 463
use-updated-eth-header 464
mka pre-shared-key 465
fallback-key 465
macsec access-control 466
replay-protection window-size 467
eapol 468
eapol destination-address 468

CHAPTER 35 Multi-Region Fabric 471
affinity-group (Multi-Region Fabric) 471
affinity-group-number 472
affinity-group preference (Multi-Region Fabric) 473
filter route outbound affinity-group preference (Multi-Region Fabric) 473
management-gateway 474
management-region 475

omp best-path region-path-length ignore (Multi-Region Fabric) 477
omp best-path transport-gateway 477
region (Multi-Region Fabric) 478
region access, region core (Multi-Region Fabric) 479
role (Multi-Region Fabric) 480
transport-gateway (Multi-Region Fabric) 481

CHAPTER 36 NAT Commands 483
ip nat 483
ip nat inside source 484
ip nat inside source tcp static interface (loopback) 488
ip nat log translations flow-export 489
ip nat outside source 490
ip nat pool 492
ip nat route vrf 493
ip nat service 494
ip nat settings preserve-sdwan-ports 495
ip nat translation (timeout) 496
ip nat translation max-entries 497
nat64 provisioning 498
nat64 route 500
nat64 settings 501
nat64 settings mtu 502
nat64 translation timeout tcp 503
nat64 translation timeout udp 503
nat66 max vpn 504
nat66 outside 505
nat66 prefix 505
nat66 route vrf 507

CHAPTER 37 NTP Commands 509
ntp access-group 509
ntp authentication-key 510
ntp server 511

ntp source 512
ntp trusted-key 512

CHAPTER 38 Object-Group Commands 515
continent 515
country 516
description (fqdn-group) 517
description (geo-group) 517
geo database 518
geo database revert 519
geo database update 519
group-object (fqdn-group) 520
group-object (geo-group) 521
object-group fqdn 521
object-group geo 522
object-group network 523
object-group security 524
object-group service 525
pattern 526

CHAPTER 39 OMP Commands 527
advertise 527
distance 529
ecmp-limit (omp) 529
graceful-restart (omp) 530
no shutdown (omp) 531
omp 532
outbound tloc-color 533
overlay-as (omp) 534
send-path-limit (omp) 535
timers 536
tloc-color-compatibility 538

CHAPTER 40 OSPF Commands 541

area nssa 541
area range 542
auto-cost 543
compatible rfc1583 543
default-information originate (OSPF) 544
distance ospf 545
max-metric router-lsa-ospf 546
router-id 547
router ospf 547
timers throttle spf 548

CHAPTER 41 **Policy Commands** 551

access-list 552
action (centralized policy) 554
action (localized policy) 556
app-agg-node 558
apply-policy 559
app-probe-class 560
app-route-policy 561
app-visibility 562
app-visibility-ipv6 563
burst 563
class (class-map) 565
cos 565
count 566
data-policy 567
default-action 567
destination-ip 568
exceed 569
flow-visibility 570
flow-visibility-ipv6 570
icmp-echo 571
implicit-acl-on-bind-intf 572
inspect 572

ip-prefix 573
ip sla 574
ip sla reaction-configuration 574
ip sla responder 576
ip sla schedule 577
ip visibility cache entries 578
ipv6 access-list 579
ipv6 visibility cache entries 579
jitter 580
lists 580
lists data-prefix-list 582
lists (tag instance) 583
loss 584
match (access-control-list) 585
match as-path 587
match (data policy) 588
match ip address 590
match protocol attribute application-group 591
parameter-map type inspect 592
policer 592
policy 594
policy ip visibility 595
policy log-rate-limit 596
queue-limit 597
rate 599
request-data-size 600
rewrite-rule 600
service-area 602
service-policy 603
set ip vrf 604
set ip next-hop verify-availability 605
sequence 606
sequence (access-control-list) 607
sla-class 608

sig 609
site-list 610
tag (IP SLA) 611
tag-instances 612
track ip sla 613
udp-jitter 614
utd-policy 615
vpn-list 615
vrf (IP SLA) 616

CHAPTER 42 PPP Commands 619
encapsulation 619
encapsulation (ATM) 620
ppp authentication 622
ppp chap hostname 623
ppp chap password 624
ppp ipcp 624
pvc 625

CHAPTER 43 PPPoEoVlan Commands 627
class (class-map) 627
dialer-group 628
dialer pool 629
encapsulation 630
interface Dialer 631
ip address 631
ip address negotiated 632
ip unnumbered 633
ppp authentication 633
ppp chap hostname 634
ppp chap password 635
ppp pap sent-username password 636
pppoe-client dial-pool-number 637
pppoe-client ppp-max-payload 638

pppoe enable group 639
protocol ppp dialer 640
set cos 641

CHAPTER 44 QoS Policy Commands 643
bandwidth 643
bandwidth (policy-map class) 644
bandwidth qos-reference 645
bandwidth remaining ratio 645
class (policy-map) 646
control-plane 647
ip nbar protocol-discovery 648
match access-group 649
match packet-tag 649
platform qos sdwan max-session 650
police (percent) 651
policy-map 652
priority 653
priority level 654
random-detect 655
service-policy 655
service-policy (policy-map class) 656
shape (policy-map class) 657
vpn packet-tag 657
platform qos port-channel-aggregate 658

CHAPTER 45 Radius Commands 659
radius-server dead-criteria 659
radius-server deadtime 660

CHAPTER 46 RIP Commands 663
address-family ipv4 vrf 664
address-family ipv6 664
auto-summary (RIP) 665

default-information originate (RIP) 666
default-metric (RIP) 666
distance (IP) 667
distribute-list (RIP) 669
distribute-list prefix-list (IPv6 RIP) 670
input-queue 671
ip rip advertise 671
ip rip receive version 672
ip rip send version 673
ipv6 prefix-list 674
ipv6 rip default-information 675
ipv6 rip enable 676
ipv6 rip metric-offset 677
ipv6 rip summary-address 677
ipv6 rip vrf-mode enable 678
ipv6 router rip 679
ipv6 unicast-routing 680
maximum-paths 680
neighbor (RIP) 681
network (RIP) 682
offset-list (RIP) 683
omp-route-tag 684
output-delay 685
passive-interface 685
redistribute 686
redistribute (IPv6) 687
router rip 688
timers basic (RIP) 689
traffic-share min 690
validate-update-source 691
version (RIP) 692

CHAPTER 47 **Routemap Commands** 693
ipv6 policy route-map 693

match ip address 694
match length 695
set community 696
route-map permit set default interface 697
route-map permit set interface 698
route-map permit set ipv6 precedence 699
set origin 700
route-map permit set vrf 701
route-map 702

CHAPTER 48 **Routing** 705
affinity-per-vrf 705
affinity-group preference-auto 706
redistribute omp translate-rib-metric 707

CHAPTER 49 **SD-WAN Tunnel Interface Commands** 709
access-list 709
allow-service 710
auto-bandwidth-detect 712
bandwidth-downstream 712
bandwidth-upstream 714
carrier 714
color 715
encapsulation 716
gre-in-udp 717
exclude-controller-group-list 718
hello-interval 719
hello-tolerance 720
iperf-server 721
last-resort-circuit 722
low-bandwidth-link 723
max-control-connections 724
nat-refresh-interval 725
port-hop 726

tloc-extension 727
tunnel-interface 727
vbond-as-stun-server 728
vmanage-connection-preference 729

CHAPTER 50 **Security Commands** 731
all-auto-sig-tunnels 731
authentication event fail 732
authentication event no-response action 733
authentication event server dead action authorize 733
authentication host-mode 734
aaa authentication dot1x 735
authentication open 735
authentication order 736
authentication port-control 736
authentication timer inactivity 737
authentication timer reauthenticate 737
authentication-type (security ipsec) 738
dot1x pae 739
dot1x system-auth-control 740
extended-ar-window 740
ip access-group 741
ipsec (security) 741
ip scp server enable 742
pairwise-keying (security ipsec) 743
pwk-sym-rekey (security ipsec) 743
rekey (security ipsec) 744
replay-window (security ipsec) 744
security 745
security ipsec integrity-type 745
sig-tunnel-list 746
switchport port-security 747
switchport port-security mac-address sticky 748

CHAPTER 51 **Service Insertion Commands** 749

service-chain 749

service-chain-affect-bfd 750

service-chain-description 751

service-chain-enable 752

service-chain-vrf 753

service 755

service service-transport-ha-pair attribute trust-posture 758

track-enable 759

CHAPTER 52 **SHDSL Commands** 761

controller SHDSL 761

dsl-group 762

firmware phy filename 764

handshake 765

ignore 766

mode (SHDSL) 767

shdsl annex 768

shdsl rate 771

shutdown (controller) 772

termination 773

CHAPTER 53 **Smart Licensing** 775

license smart transport 775

license smart url 776

CHAPTER 54 **SNMP Commands** 777

snmp ifmib ifindex persist 778

snmp mib community-map 778

snmp-server community 779

snmp-server contact 781

snmp-server context 781

snmp-server enable traps 782

snmp-server enable traps alarms informational 782
snmp-server enable traps bgp 783
snmp-server enable traps config 784
snmp-server enable traps config-copy 785
snmp-server enable traps config-ctid 785
snmp-server enable traps cpu 786
snmp-server enable traps entity 787
snmp-server enable traps entity-state 787
snmp-server enable traps event-manager 788
snmp-server enable traps flash 788
snmp-server enable traps memory 789
snmp-server enable traps ospf cisco-specific errors config-error 790
snmp-server enable traps ospf errors 790
snmp-server enable traps ospf lsa 791
snmp-server enable traps ospf state-change 792
snmp-server enable traps sdwan 793
snmp-server enable traps snmp 793
snmp-server enable traps syslog 794
snmp-server engineID local 795
snmp-server engineID remote 795
snmp-server file-transfer access-group 796
snmp-server group 797
snmp-server host 799
snmp-server location 800
snmp-server packetsize 800
snmp-server sparse-tables 801
snmp-server system-shutdown 802
snmp-server trap authentication unknown-context 803
snmp-server trap-source 804
snmp-server trap timeout 804
snmp-server user 805
snmp-server view 807
snmp trap link-status 808
tftp-server 809

CHAPTER 55 SSL Proxy Commands 811

sslproxy 811

sslproxy ca-tp-label 812

sslproxy certificate-lifetime 813

sslproxy eckey-type 814

sslproxy enable 815

sslproxy rsa-key-modulus 816

sslproxy settings certificate-revocation-check 817

sslproxy settings expired-certificate 818

sslproxy settings failure-mode 819

sslproxy settings minimum-tls-ver 820

sslproxy settings unknown-status 821

sslproxy settings untrusted-certificate 823

sslproxy settings unsupported-cipher-suites 824

sslproxy settings unsupported-protocol-versions 825

CHAPTER 56 System Commands 827

admin-tech-on-failure (system) 827

console-baud-rate 828

control-session-pps (system) 829

controller-group-list (system) 829

device-groups (system) 830

enable-ipv6-unique-local-address 830

gps-location (system) 831

logging 834

max-omp-sessions (system) 836

organization-name (system) 837

overlay-id (system) 837

port-hop (system) 838

port-offset (system) 839

site-id (system) 839

sp-organization-name (system) 840

statistics table interface collection-interval 841

system-ip (system) 841
system overlay-id 842
track-transport (system) 843
track-default-gateway (system) 843
upgrade-confirm (system) 844
vbond (system) 845

CHAPTER 57 TCP Commands 847
service tcp-keepalives-in 847
service tcp-keepalives-out 848
service tcp-small-servers 848
service udp-small-servers 849

CHAPTER 58 Tracker Commands 851
boolean 851
endpoint-api-url 853
endpoint-dns-name 853
endpoint-ip 854
endpoint-tracker 855
endpoint-tracker-settings 856
Endpoint Tracker SLA Profile 857
interval 857
icmp-interval 858
multiplier 859
threshold 860
tracker-elements 861
tracker-type 862

CHAPTER 59 Transport Gateway 867
site-type 867

CHAPTER 60 UTD Commands 869
file-analysis profile 869
file-inspection profile 871

file-reputation profile 872
flow-logging 873
logging host 874
threat-inspection profile 874
threat-inspection custom-signature profile 875
tls-decryption profile 876
utd engine standard multi-tenancy 876
utd engine standard unified-policy 877
utd global 878
utd multi-tenancy 880
web-filter url profile 881

CHAPTER 61 VDSL Commands 883
bitswap 883
controller VDSL 884
description (VDSL controller) 885
diagnostics DELT (VDSL controller) 885
firmware phy filename 886
line-mode bonding 887
line-mode single-wire line 888
modem (VDSL controller) 889
operating mode 889
sra 890
sync interval 891
sync mode (VDSL controller) 892
training log filename (VDSL controller) 893

CHAPTER 62 Voice Commands 895
allow-connections 896
bind interface 897
caller-id alerting dsp-pre-allocate 897
caller-id alerting line-reversal 898
caller-id alerting pre-ring 899
caller-id alerting ring 900

caller-id block 901
caller-id enable 902
caller-id format e911 903
caller-id mode 903
clid dtmf-codes 905
codec preference 906
credentials 907
description (dial-peer voice voip) 908
destination-pattern 908
dial-peer voice (VOIP) 910
dtmf-relay (VOIP) 910
hunt-scheme least-used 911
hunt-scheme round-robin 912
hunt-scheme sequential 913
id network 913
keepalive retries 914
keepalive timeout 915
max-dn 915
max-pool 916
registrar server 916
security-policy (voice register global) 917
session protocol 918
session-transport 919
sccp ip precedence 920
system message (voice register global) 920
sip 921
sip-ua 921
supplementary-service sip 922
translation-profile (voice register) 923
voice-class codec (voice register pool) 924
voice-class codec (dial peer voice) 925
voice class codec 925
voice register global 926
voice register pool 927

voice service voip 927

CHAPTER 63 VRF Commands 929

address-family ipv4 929

address-family ipv6 931

description (VRF definition) 932

ip vrf 932

platform ipreass boost-mode 933

rd (VPLS) 933

redistribute vrf 934

route-replicate (VRF address family) 937

route-target 938

service tcp-keepalives-in 939

service tcp-keepalives-out 940

service tcp-small-servers 940

service udp-small-servers 941

vrf definition 941

CHAPTER 64 VRRP Commands 943

object (tracking) 943

track interface 944

track list 945

track (VRRP) 947

track service 948

tloc-change increase-preference 948

vrf forwarding 949

vrrp address-family 950

CHAPTER 65 Zone Based Firewall Commands 951

alert (zone-based policy) 951

app-visibility 952

class-map 953

class-map type inspect 954

class (policy-map) 955

drop 956
flow-visibility 957
implicit-acl-logging 958
inspect 958
log (parameter-map type) 959
log flow-export 959
log-frequency 960
match access-group 961
multi-tenancy 961
parameter-map type inspect-global 962
policy 963
policy-map type inspect 965
service-policy (zones) 966
service-policy type inspect 966
vpn zone security 967
vpn (zone) 968
zone pair security 968
zone security 969

CHAPTER 66 Zscaler Commands 971

aup 971
auth-required 972
caution-enabled 973
datacenters 973
ips-control 974
ofw-enabled 974
secure-internet-gateway 975
ssl-scan-enabled 976
surrogate display-time-unit 977
surrogate idle-time 977
surrogate ip 978
surrogate ip-enforced-for-known-browsers 979
surrogate refresh-time 980
surrogate refresh-time-unit 980

tunnel-options 981

xff-forward-enabled 982

zscaler-location-settings 983

CHAPTER 67 **Troubleshooting Commands** 985

clear ip nat statistics 992

clear sdwan app-fwd cflowd flow-all 993

clear sdwan app-fwd cflowd statistics 993

clear sdwan app-route statistics 994

clear sdwan appqoe dreopt 995

clear sdwan bfd transitions 995

clear sdwan control connection-history 996

clear sdwan control connections 997

clear sdwan control port-index 998

clear sdwan dns app-fwd cflowd flow-all 998

clear sdwan dns app-fwd cflowd statistics 999

clear sdwan dns app-fwd dpi flow-all 1000

clear sdwan dns app-fwd dpi summary 1000

clear sdwan dns app-route statistics 1001

clear sdwan dns cache 1001

clear sdwan installed-certificates 1002

clear sdwan notification stream viptela 1003

clear sdwan omp 1003

clear sdwan policy 1004

clear sdwan reverse-proxy context 1005

clear sdwan tunnel gre-keepalive 1006

clear sdwan tunnel statistics 1007

clear sdwan umbrella dp-stats 1007

clear sdwan utd engine standard logging events 1008

clear sdwan utd engine standard statistics daq vrf 1008

clear sdwan utd engine standard statistics url-filtering vrf 1009

clear sdwan utd statistics 1010

clear sdwan zbfw statistics drop 1011

debug packet-trace condition 1012

debug platform condition match 1013
debug platform condition start 1014
debug platform condition stop 1014
debug platform condition feature sdwan controlplane bfd 1015
debug platform software sdwan fpm 1015
debug vdaemon 1016
debug platform software sdwan vdaemon 1018
set platform software trace 1019
set platform software trace vdaemon 1020
show sdwan control connections 1021
monitor capture (access list/class map) 1022
monitor capture (interface/control plane) 1024
monitor capture match ipv4 1025
monitor capture match ipv6 1025
privilege exec level 1027
request nms sdavc-gw 1028
request nms patch all 1029
request nms unpatch 1031
request nms container-manager diagnostics 1032
request platform software sdwan admin-tech 1035
request platform software sdwan auto-suspend reset 1036
request platform software sdwan certificate install 1037
request platform software sdwan config reset 1038
request platform software sdwan csr upload 1039
request platform software sdwan port_hop color 1040
request platform software sdwan root-cert-chain install 1041
request platform software sdwan root-cert-chain uninstall 1042
request platform software sdwan software activate 1042
request platform software sdwan software install 1043
request platform software sdwan software remove 1044
request platform software sdwan software secure-boot 1045
request platform software sdwan software set-default 1045
request platform software sdwan software upgrade-confirm 1046
set platform software trace 1047

show platform software sdwan interface-alarm summary 1055
show aaa servers 1056
show autoip status 1056
show class map type inspect 1057
show cellular 1058
show clock 1059
show config-pull history 1060
Show config-pull transactions 1061
show configuration commit list 1066
show crypto ipsec sa 1067
show cts environment-data 1072
show cts pac 1073
show cts role-based counters 1074
show cts role-based permissions 1075
show cts role-based sgt-map 1076
show cts sxp connections 1077
show crypto key mypubkey rsa 1079
show crypto ikev2 stats 1080
show crypto pki certificates 1081
show crypto session 1084
show endpoint-tracker 1085
show etherchannel load-balancing 1089
show etherchannel summary 1089
show flow exporter 1090
show flow monitor sdwan_flow_monitor cache 1097
show flow record 1098
show full-configuration probe-path load-balance-dia 1099
show geo file-contents info 1100
show geo status 1100
show interfaces 1101
show interface port-channel 1105
show interface port-channel etherchannel 1107
show inventory 1108
show idmgr status 1110

show idmgr omp ip-user-bindings 1111
show idmgr omp user-usergroup-bindings 1111
show idmgr user-sessions 1112
show ip bgp ipv4 1113
show ip bgp vpnv4 1115
show ip bgp vpnv4 vrf 1124
show ip dhcp binding 1125
show ip cef vrf 1126
show ip msdp vrf count 1127
show ip msdp vrf peer 1127
show ip msdp vrf sa-cache 1128
show ip msdp vrf summary 1129
show ip interface 1129
show ip interface brief 1132
show ip nat redundancy 1133
show ip nat route-dia 1134
show ip nat statistics 1134
show ip nat translations 1136
show ip nat status 1139
show running nat 1140
show ip pim bsr-router 1141
show ip pim rp 1141
show ip protocols 1142
show ip rip database 1145
show ip rip neighbors 1146
show ip route 1147
show ip route rip 1157
show ip route vrf 1158
show ip sla summary 1162
show ipv6 access-list 1163
show ipv6 dhcp binding 1163
show ipv6 dhcp database 1164
show ipv6 dhcp interface 1165
show ipv6 dhcp pool 1166

show ipv6 route vrf 1167
show key chain 1168
show lacp 1168
show lte450 all 1170
show lte450 network 1172
show lte450 hardware 1173
show lte450 radio 1174
show logging cacert 1175
show logging profile sdwan internal filter 1175
show macsec hw detail 1177
show macsec mka-request-notify 1178
show macsec summary 1178
show macsec status interface 1179
show mka default-policy 1180
show mka keychains 1183
show mka policy 1183
show mka sessions 1184
show mka statistics 1187
show mka summary 1187
show nat66 dia route 1189
show nat64 map-e 1190
show nat66 nd 1190
show nat66 prefix 1191
show nat66 statistics 1192
show object-group 1192
show policy-firewall session platform detail 1193
show performance monitor cache 1194
show performance monitor context 1195
show platform hardware qfp active classification class-group-manager class-group client cce name 1199
show platform hardware qfp active classification class-group-manager class-group client sdwan 1200
show platform hardware qfp active classification class-group-manager object-group 1201
show platform hardware qfp active classification feature message all 1203
show platform hardware qfp active classification feature-manager exmem-usage 1204
show platform hardware qfp active classification feature-manager statistics 1205

show platform hardware qfp active feature acl control 1206
show platform hardware qfp active feature acl dp hsl configuration 1208
show platform hardware qfp active feature acl dp hsl statistics 1210
show platform hardware qfp active feature bfd datapath 1211
show platform hardware qfp active feature bfd datapath 1213
show platform hardware qfp active feature firewall drop 1215
show platform hardware qfp active feature geo client 1216
show platform hardware qfp active feature geo datapath 1217
show platform hardware qfp active feature nat datapath hsl 1218
show platform hardware qfp active feature nat datapath map 1219
show platform hardware qfp active feature nat datapath sess-dump 1220
show platform hardware qfp active feature nat datapath stats 1221
show platform hardware qfp active feature nat datapath summary 1221
show platform hardware qfp active feature nat66 datapath prefix 1223
show platform hardware qfp active feature nat66 datapath statistics 1224
show platform hardware qfp active feature sdwan client phy-wan-bind-list 1224
show platform hardware qfp active feature utd config 1225
show platform hardware qfp active interface if-name 1226
show platform hardware qfp active statistics drop 1227
show platform hardware qfp active feature firewall datapath rg 1228
show platform hardware qfp active feature firewall drop all 1231
show platform hardware qfp active feature bridge-domain datapath sdwan-flood-list 1233
show platform packet-trace 1234
show platform packet-trace fia-statistics 1236
show platform software common-classification f0 tag 1237
show platform software cpu alloc 1239
show platform software ipsec fp active flow 1241
show platform software ipsec ftm-msg-stats 1245
show platform software ipsec sdwanrp-msg-stats 1246
show platform software ipsec vesen-event-log 1247
show platform software memory 1248
show platform software nat66 fp active 1250
show platform software nat66 rp active 1251
show platform software sdwan ftmd bridge-domain 1252

show platform software sdwan multicast active-sources vrf 1253
show platform software sdwan multicast remote-nodes vrf 1253
show platform software sdwan qos 1254
show platform software sdwan tloc-db 1256
show platform software sdwan ttmd local-tlocs 1257
show platform software sdwan ttmd history tloc 1258
show platform software sdwan ttmd tlocs stats 1259
show policy-firewall config 1259
show policy-map interface Port-channel 1260
show processes cpu platform 1262
show policy-map type inspect 1264
show power 1264
show raw-socket 1266
show redundancy application control-interface group 1267
show redundancy application data-interface group 1268
show redundancy application group 1269
show redundancy application group protocol 1272
show redundancy rii 1273
show sd-routing certificate staged 1274
show sdwan alarms detail 1275
show sdwan alarms summary 1276
show sdwan appqoe 1277
show sdwan appqoe dreopt 1281
show sdwan appqoe dreopt statistics 1283
show sdwan appqoe error recent 1284
show sdwan appqoe flow closed all 1288
show sdwan appqoe flow closed flow-id 1289
show sdwan appqoe flow flow-id 1294
show sdwan appqoe flow vpn-id 1299
show sdwan appqoe status 1300
show sdwan app-fwd cflowd collector 1301
show sdwan app-fwd cflowd flows 1302
show sdwan app-fwd cflowd flow-count 1304
show sdwan app-fwd cflowd statistics 1305

show sdwan app-fwd cflowd template 1306
show sdwan app-fwd dpi flows 1307
show sdwan app-fwd dpi summary 1310
show sdwan app-route sla-class 1311
show sdwan app-route stats 1312
show sdwan bfd history 1316
show sdwan bfd sessions 1317
show sdwan bfd sessions region-access 1319
show sdwan bfd sessions region-core 1320
show sdwan bfd summary 1320
show sdwan bfd tloc-summary-list 1322
show sdwan certificate 1323
show sdwan certificate staged 1328
show sdwan cloudexpress applications 1329
show sdwan cloudexpress gateway-exits 1331
show sdwan cloudexpress load-balance applications 1333
show sdwan cloudexpress local-exits 1335
show sdwan control 1336
show sdwan debugs 1342
show sdwan firmware-packages details 1344
show sdwan firmware-packages list 1344
show sdwan from-vsmart commit-history 1345
show sdwan from-vsmart policy 1347
show sdwan from-vsmart tag-instances 1349
show sdwan ftm umts 1350
show sdwan ftm umts logs 1351
show sdwan geofence-status 1352
show sdwan interface color 1353
show sdwan ipsec inbound-connections 1353
show sdwan ipsec local-sa 1355
show sdwan ipsec outbound-connections 1356
show sdwan ipsec pwk inbound-connections 1357
show sdwan ipsec pwk local-sa 1359
show sdwan ipsec pwk outbound-connections 1360

show sdwan nat-fwd ip-nat-translation 1362
show sdwan nat-fwd ip-nat-translation-verbose 1363
show sdwan omp cloudexpress 1364
show sdwan omp ipv6-routes 1366
show sdwan omp multicast-auto-discover 1368
show sdwan omp multicast-routes 1369
show sdwan omp peers 1370
show sdwan omp routes 1374
show sdwan omp l2-routes 1379
show sdwan omp services 1385
show sdwan omp summary 1386
show sdwan omp tlocs 1389
show sdwan policy access-list-associations 1396
show sdwan policy access-list-counters 1397
show sdwan policy access-list-names 1397
show sdwan policy access-list-policers 1398
show sdwan policy app-route-policy-filter 1398
show sdwan policy data-policy-filter 1400
show sdwan policy from-vsmart 1402
show sdwan policy ipv6 access-list-associations 1403
show sdwan policy ipv6 access-list-counters 1404
show sdwan policy ipv6 access-list-names 1405
show sdwan policy ipv6 access-list-policers 1405
show sdwan policy rewrite-associations 1406
show sdwan reboot history 1407
show sdwan running-config 1408
show sdwan security-info 1411
show sdwan secure-internet-gateway tunnels 1411
show sdwan secure-internet-gateway umbrella tunnels 1413
show sdwan secure-internet-gateway zscaler tunnels 1414
show sdwan software 1415
show platform software sdwan dta cflowd statistics 1416
show sdwan system status 1417
show sdwan tag-instances from-vsmart 1420

show sdwan version 1421
show sdwan zbfw drop-statistics 1421
show sdwan zbfw zonepair-statistics 1423
show sdwan zonebfwdp sessions 1424
show service-insertion type appqoe 1426
show sslproxy statistics 1428
show sslproxy status 1429
show standby 1431
show standby neighbors 1435
show support policy route-policy 1437
show tech-support sdwan bfd 1438
show track 1442
show uidp statistics 1444
show uidp user-group all 1445
show uidp user ip 1446
show utd engine standard config 1446
show utd unified-policy 1448
show vrrp 1449
show wireless-bridge status 1452
show wireless-lan radio 1453
show wireless-lan wlan 1453
show wireless-lan client 1454
show zone-pair security 1455
verify 1455
vdiagnose vmanage cluster 1456

CHAPTER 68 **Wireless Commands** 1459

passphrase 1459
data-security 1460
qos-type 1461
radio-profile 1461
ssid 1462
wireless-lan country 1463
wireless-lan mgmt 1463

wlan-profile 1464

CHAPTER 69 **Commands Qualified in Cisco IOS XE Catalyst SD-WAN Release 17.x** 1465

Qualified CLIs for Cisco IOS XE Catalyst SD-WAN Release 17.2.1r 1465

Qualified CLIs for Cisco IOS XE Release Amsterdam 17.2.1v 1467

Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.3.1a 1485

Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.4.1a 1497

Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.5.1a 1507

Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.6.1a 1514

Qualified Commands for Cisco IOS XE Release 17.6.4 1526

Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.7.1a 1526

Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.8.1a 1532

Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.9.1a 1534

Qualified Commands for Cisco IOS XE Release 17.10.1a 1535

Qualified Commands for Cisco IOS XE Release 17.11.1a 1537

Qualified Commands for Cisco IOS XE Release 17.12.1a 1541

Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.13.1a 1543

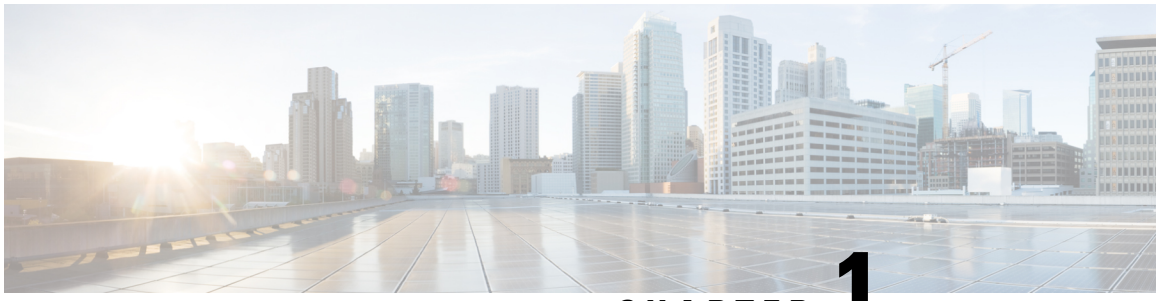
Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.14.1a 1544

Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.15.1a 1545

Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.16.1a 1546

Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.18.1a 1546

Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 26.1.1 1547



CHAPTER 1

Read Me First

Note To achieve simplification and consistency, the Cisco SD-WAN solution has been rebranded as Cisco Catalyst SD-WAN. In addition, from Cisco IOS XE SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Release 20.12.1, the following component changes are applicable: **Cisco vManage** to **Cisco Catalyst SD-WAN Manager**, **Cisco vAnalytics** to **Cisco Catalyst SD-WAN Analytics**, **Cisco vBond** to **Cisco Catalyst SD-WAN Validator**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

Related References

- Cisco Catalyst SD-WAN Control Components Compatibility Matrix and Server Recommendations
- Cisco Catalyst SD-WAN Device Compatibility

User Documentation

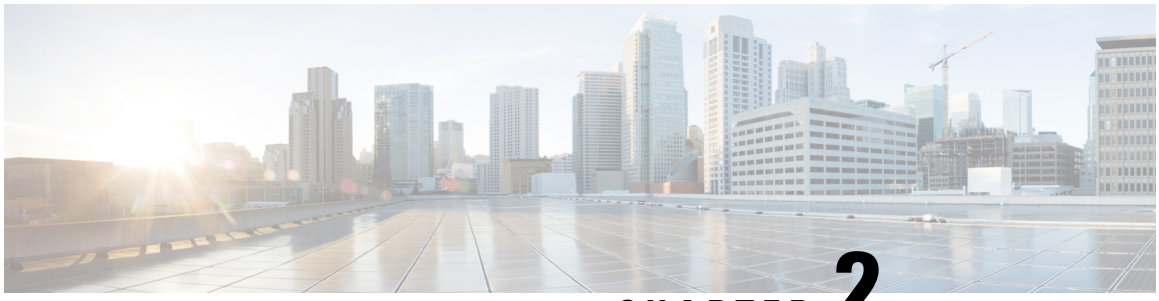
- User Documentation for Cisco IOS XE Catalyst SD-WAN Release 17

Communications, Services, and Additional Information

- Sign up for Cisco email newsletters and other communications at: Cisco Profile Manager.
- For information on the latest technical, advanced, and remote services to increase the operational reliability of your network visit Cisco Services.
- To browse and discover secure, validated enterprise-class apps, products, solutions, and services, visit Cisco Devnet.
- To obtain general networking, training, and certification titles from Cisco Press Publishers, visit Cisco Press.
- To find warranty information for a specific product or product family, visit Cisco Warranty Finder.
- To view open and resolved bugs for a release, access the Cisco Bug Search Tool.
- To submit a service request, visit Cisco Support.

Documentation Feedback

To provide feedback about Cisco technical documentation use the feedback form available in the right pane of every online document.

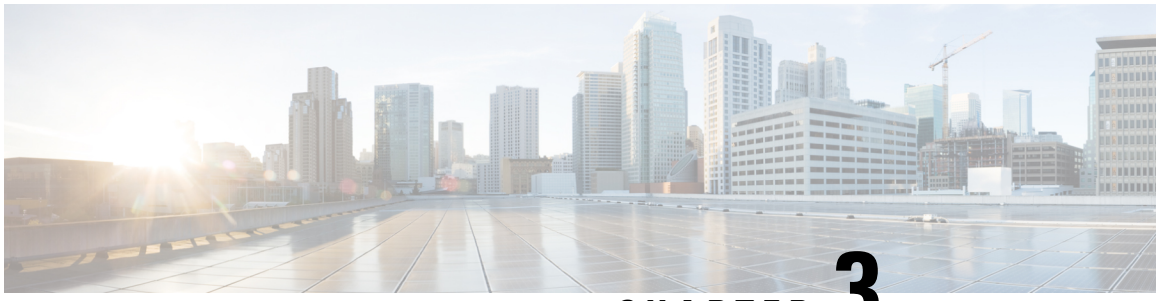


CHAPTER 2

What's New in Cisco IOS XE (Catalyst SD-WAN)

What's New in Cisco IOS XE Catalyst SD-WAN Release 17.x

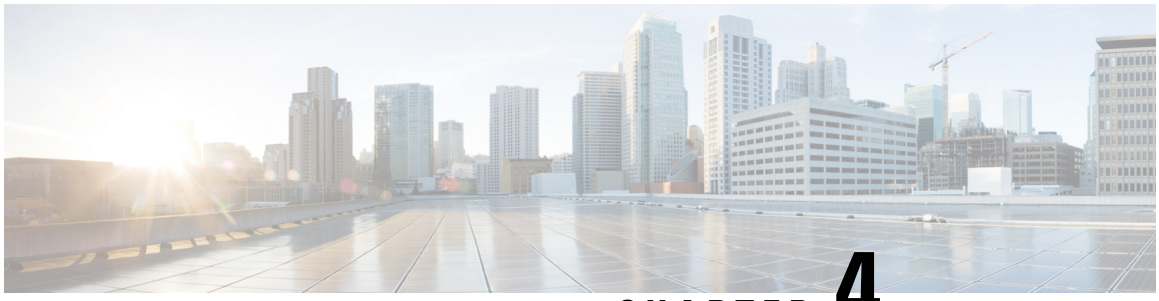
What's New in Cisco SD-WAN (vEdge) Release 20.x



CHAPTER 3

Introduction

This document contains a technology-group based alphabetical listing of commands. These commands are qualified for use with CLI templates in Cisco vManage. To search for a command, use the alphabet key in the relevant technology chapter and scroll down until you find the command of interest, or use the Find function in the PDF format. For more information on CLI templates, refer CLI Templates for Cisco IOS XE SD-WAN Routers.



CHAPTER 4

AAA Commands

- aaa accounting, on page 7
- aaa authentication attempts login, on page 10
- aaa authentication enable default, on page 10
- aaa authentication login, on page 11
- aaa authentication password-prompt, on page 13
- aaa authentication ppp, on page 13
- aaa authentication username-prompt, on page 14
- aaa authorization, on page 15
- aaa authorization config-commands, on page 16
- aaa authorization console, on page 17
- aaa authorization credential download default, on page 18
- aaa lockout-policy, on page 19
- aaa group server tacacs+, on page 20
- aaa netconf-accounting, on page 20
- ip tacacs source-interface, on page 21
- ip vrf forwarding (server-group), on page 22
- lockout-policy, on page 23
- login block-for, on page 25
- login quiet-mode access-class, on page 26
- login-rate, on page 27
- multi-factor-auth duo, on page 27
- server-private (TACACS+), on page 29
- tacacs server address ipv4, on page 30
- tacacs server key, on page 31
- tacacs server port, on page 31
- tacacs server timeout, on page 32

aaa accounting

To enable authentication, authorization, and accounting (AAA) accounting of requested services for billing or security purposes when you use TACACS+, use the **aaa accounting** command in global configuration mode or template configuration mode. To disable AAA accounting, use the **no** form of this command.

aaa accounting { **system** | **exec** | **network** | **connection** *connection-name* | **commands** *level* } [**default**] { **start-stop** | **stop-only** } **group** *group-name*
no aaa accounting { **system** | **exec** | **connection** *connection-name* | **commands** *level* } [**default**] { **start-stop** | **stop-only** } **group** *group-name*

Syntax Description

system	Performs accounting for all system-level events not associated with users, such as reloads. **Note** When system accounting is used and the accounting server is unreachable at system startup time, the system will not be accessible for approximately two minutes.
commands **connection** **exec**	Specifies the accounting method list. Enter at least one of the following keywords: • **commands**: Creates a method list to provide accounting information about specific, individual EXEC commands associated with a specific privilege level. • **connection**: Creates a method list to provide accounting information about all outbound connections made from the network access server. • **exec**: Creates a method list to provide accounting records about user EXEC terminal sessions on the network access server, including username, date, and start and stop times.
exec	Runs accounting for the EXEC shell session. This keyword might return user profile information such as what is generated by the **autocommand** command.
network	Runs accounting for all network-related service requests.
connection	Provides information about all outbound connections made from the network access server, such as Telnet, local-area transport (LAT), TN3270, packet assembler and disassembler (PAD), and rlogin.
commands *level*	Runs accounting for all commands at the specified privilege level. Valid privilege level entries are integers from 0 through 15.
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 record for all cases including authentication failures regardless of whether the **aaa accounting send stop-record authentication failure** command is configured.
group *group-name*	Server groups for aaa accounting with *group-name* as character string or radius or tacacs+ as defined by **aaa group server** command.

Command Default

AAA accounting is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1r	Command qualified for use in Cisco vManage CLI templates. **exec**, **commands**, **connection**, **system** keywords and **group** *group-name*, **local** , **none** methods are supported.
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Additional method qualified: **network**
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	Support for multi-group configuration is added.
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	Additional methods qualified: **group tacacs+**

Usage Guidelines

Use the **aaa accounting** command to enable accounting and to create named method lists that define specific accounting methods on a per-line or per-interface basis.

For usage guidelines, see the Cisco IOS XE aaa accounting command.

The table below contains descriptions of keywords for AAA accounting methods.

Table 1: aaa accounting Methods

Keyword	Description
group *group-name*	Uses a subset of RADIUS or TACACS+ servers for accounting as defined by the server group *group-name* argument.
group tacacs+	Uses the list of all TACACS+ servers for authentication as defined by the **aaa group server tacacs+** command.

Examples

The following example shows how to define a default command accounting method list, where accounting services are provided by a TACACS+ security server, set for privilege level 15 commands with a stop-only restriction:

```
aaa accounting commands 15 default stop-only group tacacs+

aaa authorization commands 15 default local group tacacs+

aaa accounting exec default start-stop group tacacs+

aaa accounting commands 15 default start-stop group tacacs+

aaa accounting system default start-stop group tacacs+

aaa accounting network default group tacacs+
```

The following example shows how to configure multiple groups:

```
aaa accounting commands 15 default start-stop group tacacs+ broadcast logger group radius
```

aaa authentication attempts login

To set the maximum number of login attempts that will be permitted before a session is dropped, use the **aaa authentication attempts login**command in global configuration mode. To reset the number of attempts to the default, use the **no** form of this command.

aaa authentication attempts login *number-of-attempts*
no aaa authentication attempts login

Syntax Description

number-of-attempts	Number of login attempts. Range is from 1 to 25. Default is 3.

Command Default

3 attempts

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE SD-WAN Release 17.2.1r	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

The **aaa authentication attempts login** command configures the number of times a router will prompt for username and password before a session is dropped.

Examples

The following example configures a maximum of 5 attempts at authentication for login:

```
aaa authentication attempts login 5
```

aaa authentication enable default

To enable authentication, authorization, and accounting (AAA) authentication to determine whether a user can access the privileged command level, use the **aaa authentication enable default** command in global configuration mode. To disable this authorization method, use the **no** form of this command.

aaa authentication enable default *method1* [*method2* . . .]
no aaa authentication enable default *method1* [*method2* . . .]

Syntax Description

method1 [*method2...*]	At least one of the keywords described in the table below.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.18.1a	Command qualified for use in Cisco vManage CLI templates. **group** *group-name* and **enable** keywords are supported.

Usage Guidelines

Use the **aaa authentication enable default** command to create a series of authentication methods that are used to determine whether a user can access the privileged command level. Method keywords are described in the table below. The additional methods of authentication are used only if the previous method returns an error, not if it fails.

For usage guidelines, see the Cisco IOS XE aaa authentication enable default command.



Note To prevent being locked out in User EXEC mode when the command **aaa authentication enable default enable** is present in the running or startup configuration, configure an enable password on the device.

Table 2: aaa authentication enable default Methods

Keyword	Description
enable	Uses the enable password for authentication. **Note** An authentication request fails over to the next authentication method only if no enable password is configured on the router.
group tacacs+	Uses the list of all TACACS+ servers for authentication.
group *group-name*	Uses a subset of TACACS+ servers for authentication as defined by the **aaa group server tacacs+** command.

Examples

```
aaa authentication enable default group tacacs-511 enable
```

aaa authentication login

To set authentication, authorization, and accounting (AAA) authentication at login, use the **aaa authentication login** command in global configuration mode. To disable AAA authentication, use the **no** form of this command.

aaa authentication login { **default** *list-name* } *method1* [*method2* . . .]
no aaa authentication login { **default** *list-name* } *method1* [*method2* . . .]

Syntax Description

default	Uses the listed authentication methods that follow this keyword as the default list of methods when a user logs in.
list-name	Character string used to name the list of authentication methods activated when a user logs in. See the “Usage Guidelines” section for more information.

method1 [*method2...*]	The list of methods that the authentication algorithm tries in the given sequence. You must enter at least one method; you may enter up to four methods. Method keywords are described in the table below.

Command Default

AAA authentication at login is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE SD-WAN Release 17.2.1r	Command qualified for use in Cisco vManage CLI templates. **default**, **group** *group-name* keyword-argument pair are supported.
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	Additional parameters qualified: , **group tacacs+**, and **local** keywords were added as methods for authentication.

Usage Guidelines

If the **default** keyword is not set, only the local user database is checked. This has the same effect as the following command:

```
aaa authentication login default local
```

Note On the console, login will succeed without any authentication checks if **default** keyword is not set.

For usage guidelines, see the Cisco IOS XE aaa authentication login command.

The table below describes the method keywords.

Table 3: aaa authentication login Methods Keywords

Keyword	Description
enable	Uses the enable password for authentication. This keyword cannot be used.
group *group-name*	Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the **aaa group server tacacs+** command.
group tacacs+	Uses the list of all TACACS+ servers for authentication.
local	Uses the local username database for authentication.

```
aaa authentication login default group tacacs+ local
```

```
aaa authentication login default group tacacs-511
```

aaa authentication password-prompt

To change the text displayed when users are prompted for a password, use the **aaa authentication password-prompt** command in global configuration mode. To return to the default password prompt text, use the **no** form of this command.

aaa authentication password-prompt *text-string*
no aaa authentication password-prompt *text-string*

Syntax Description

text-string	String of text that will be displayed when the user is prompted to enter a password. If this text-string contains spaces or unusual characters, it must be enclosed in double-quotes (for example, “Enter your password:”).

Command Default

There is no user-defined *text-string*, and the password prompt appears as “Password.”

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Release 17.3.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE aaa authentication password-prompt command.

Examples

The following example changes the text for the password prompt:

```
aaa authentication password-prompt “Enter your password now:”
```

aaa authentication ppp

To specify one or more authentication, authorization, and accounting (AAA) methods for use on serial interfaces that are running PPP, use the **aaa authentication ppp** command in global configuration mode. To disable authentication, use the **no** form of this command.

aaa authentication ppp *list-name method1*
no aaa authentication ppp *list-name method1*

Syntax Description

list-name	Character string used to name the list of authentication methods tried when a user logs in.
method1	Identifies the list of methods that the authentication algorithm tries in the given sequence. You must enter at least one method; you may enter up to four methods. Method keywords are described in the table below.

Command Default

AAA authentication methods on serial interfaces running PPP are not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 17.3.1a	Command qualified for use in Cisco vManage CLI templates. **local** keyword is supported.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE aaa authentication ppp command.

Table 4: aaa authentication ppp Methods

Keyword	Description
local	Uses the local username database for authentication.

Examples

The following example shows how to create a AAA authentication list called *dialinppp* for serial lines that use PPP. This authentication first tries to contact a TACACS+ server. If this action returns an error, the user is allowed access with no authentication.

```
aaa authentication ppp dialinppp local
```

aaa authentication username-prompt

To change the text displayed when users are prompted to enter a username, use the **aaa authentication username-prompt** command in global configuration mode. To return to the default username prompt text, use the **no** form of this command.

aaa authentication username-prompt *text-string*
no aaa authentication username-prompt *text-string*

Syntax Description

text-string	String of text that will be displayed when the user is prompted to enter a username. If this text-string contains spaces or unusual characters, it must be enclosed in double-quotes (for example, “Enter your name:”).

Command Default

There is no user-defined *text-string*, and the username prompt appears as “Username.”

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Release 17.3.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

Use the **aaa authentication username-prompt** command to change the default text that the Cisco IOS software displays when prompting a user to enter a username. The **no** form of this command returns the username prompt to the default value:

```
Username:
```

Some protocols (for example, TACACS+) have the ability to override the use of local username prompt information. Using the **aaa authentication username-prompt** command will not change the username prompt text in these instances.



Note The **aaa authentication username-prompt** command does not change any dialog that is supplied by a remote TACACS+ server.

Examples

The following example changes the text for the username prompt:

```
aaa authentication username-prompt "Enter your name here:"
```

aaa authorization

To set the parameters that restrict user access to a network, use the **aaa authorization** command in global configuration mode. To remove the parameters, use the **no** form of this command.

aaa authorization { **commands** *level* | **exec** | **network** } { **default** *list-name* } [*method1* [*method2* . . .]]
no aaa authorization { **commands** *level* | **exec** | **network** } { **default** *list-name* } [*method1* [*method2* . . .]]

Syntax Description

commands	Runs authorization for all commands at the specified privilege level.
level	Specific command level that should be authorized. Valid entries are 0 through 15.
exec	Runs authorization to determine if the user is allowed to run an EXEC shell. This facility returns user profile information such as the autocommand information.
network	Runs authorization for all network-related service requests, including Serial Line Internet Protocol (SLIP), PPP, PPP Network Control Programs (NCPs), and AppleTalk Remote Access (ARA).
default	Uses the listed authorization methods that follow this keyword as the default list of methods for authorization.
list-name	Character string used to name the list of authorization methods.
method1 [*method2...*]	(Optional) Identifies an authorization method or multiple authorization methods to be used for authorization. A method may be any one of the keywords listed in the table below.

Command Default

Authorization is disabled for all actions.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE SD-WAN Release 17.2.1r	Command qualified for use in Cisco vManage CLI templates. **config-commands**, **exec**, **command**, **network**, **default** keywords and **group** *group-name*, **local** , **none** methods are supported
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	Additional methods qualified: **group tacacs+**

Usage Guidelines

For usage guidelines, see the Cisco IOS XE aaa authorization command.

The table below describes the method keywords.

Table 5: aaa authorization Methods

Keyword	Description
group *group-name*	Uses a subset of RADIUS or TACACS+ servers for accounting as defined by the **aaa group server** *group-name* command.
group tacacs+	Uses the list of all TACACS+ servers for authorization as defined by the **aaa group server tacacs**+ command.
local	Uses the local database for authorization.
none	Indicates that no authorization is performed.

Examples

The following example shows how to define aaa authorization:

```
aaa authorization commands 15 default local group tacacs+
aaa authorization network default local
aaa authorization commands 2 default group tacacs-511 local none
```

aaa authorization config-commands

To reestablish the default created when the **aaa authorization commands** command was issued, use the **aaa authorization config-commands** command in global configuration mode. To disable authentication, authorization, and accounting (AAA) configuration command authorization, use the **no** form of this command.

aaa authorization config-commands
no aaa authorization config-commands

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 Catalyst SD-WAN Release 17.12.1a	Command qualified for use in Cisco vManage CLI template

Usage Guidelines

For usage guidelines, see the Cisco IOS XE aaa authorization config-commands command.

Examples

The following example specifies that TACACS+ authorization is run for level 15 commands and that AAA authorization of configuration commands is disabled:

```
aaa authorization command 15 group tacacs+ none
no aaa authorization config-commands
```

aaa authorization console

To apply authorization to a console, use the **aaa authorization console** command in global configuration mode. To disable the authorization, use the **no** form of this command.

aaa authorization console
no aaa authorization console

Syntax Description

This command has no arguments or keywords.

Command Default

Authentication, authorization, and accounting (AAA) authorization is disabled on the console.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Release 17.3.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE aaa authorization console command.

Examples

The following example shows that the default authorization that is configured on the console line is being disabled:

```
Router (config)# aaa authorization console
```

aaa authorization credential download default

To set an authorization method list to use local credentials, use the **aaa authorization credential download default** command in global configuration mode. To disable the authorization method list from using the local credentials, use the **no** form of this command.

aaa authorization credential download { **default** | **auth_list** } [**cache**] [**group**] [**if-authenticated**] [**local**] [**none**] [**radius**] [**tacacs**]
no aaa authorization credential download { **default** | **auth_list** }

Syntax Description

default	Specifies the authorization methods that follow the default list.
auth_list	Specifies the named authorization method list.
cache	(Optional) Uses a cache server group for authorization.
group	(Optional) Uses a subset of RADIUS or TACACS+ servers for accounting as defined by the **aaa group server group-name** command.
if-authenticated	(Optional) Allows the user to access the requested function if the user is authenticated. **Note** The **if-authenticated** method is a terminating method. Therefore, if it is listed as a method, any methods listed after it will never be evaluated.
local	(Optional) Uses the local database for authorization.
none	(Optional) Indicates that no authorization is performed.
radius	(Optional) Uses RADIUS for authorization.
tacacs	(Optional) Uses TACACS+ for authorization.

Command Default

Disabled, unless the **aaa authorization** command is configured, in which case all config-commands require authorization.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	This command was introduced.

Usage Guidelines

Use the **aaa authorization credential-download** command for downloading EAP credentials from the local database or from the RADIUS, or LDAP server as defined by aaa group server command.

Examples

The following example shows how to set an authorization method list to use local credentials:

```
Device(config)# aaa authorization credential-download default local
```

The following example shows how to configure four groups to set an authorization method list:

```
Device(config)# aaa authorization credential-download Ap-Auth group radius-group cache ldap
 local if-authenticated
```

aaa lockout-policy

To configure the authentication, authorization, and accounting (AAA) user lockout policy in system configuration mode for Cisco SD-WAN Manager, use the **aaa lockout-policy** command in system configuration mode.

To disable the system lockout policy, use the **no** form of this command.

aaa lockout-policy **fail-attempts** *attempt-count* **fail-interval** *fail-int* **lockout-interval** *lockout-int*

no aaa lockout-policy

Syntax Description

fail-attempts *attempt-count*	Specifies the number of failed authentication attempts before the user is locked out. Default: 5 Range: 1 - 3600
fail-interval *fail-int*	Specifies the duration in seconds of failed authentication attempts before the user is locked out. Default: 900 Range: 1 - 3600
lockout-interval *lockout-int*	Specifies the lockout duration in seconds. Default: 900 Range: 1 - 3600

Command Modes

system configuration (config-system)

Command History

Command History

Release	Modification
Cisco Catalyst SD-WAN Control Components Release 20.12.1	This command is supported in Cisco SD-WAN.

Usage Guidelines

Use the **aaa lockout-policy** command to configure notifications for unauthorized activity.

Examples

The following example shows how to configure the lockout policy:

```
sdwan-manager(config)# system
sdwan-manager(config-system)# aaa
```

```
sdwan-manager(config-aaa)# lockout-policy lockout-interval 600 fail-interval 60 fail-attempts
 5
```

In the above example, **fail-attempts** is 5, **fail-interval** is 60, and **lockout-interval** is 600. The result is that if there are 5 failed attempts to log in within 60 seconds, then the Cisco SD-WAN Manager does not allow additional attempts for a period of 600 seconds (10 minutes).

aaa group server tacacs+

To group different TACACS+ server hosts into distinct lists and distinct methods, use the **aaa group server** tacacs+ command in global configuration mode. To remove a server group from the configuration list, use the **no** form of this command.

aaa group server tacacs+ *group-name*
no aaa group server tacacs + *group-name*

Syntax Description

group-name	Character string used to name the group of servers. See the table below for a list of words that cannot be used as the *group-name* argument.

Command Default

No default behavior or values.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE 17.2.1r	Command qualified for use in Cisco vManage templates.

Usage Guidelines

For usage guidelines, refer to Cisco IOS XE aaaa group server tacacs+ command.

Examples

The following example shows the configuration of an AAA server group named tacgroup1 that comprises three member servers:

```
aaa group server tacacs+ tacgroup1
server 10.1.1.1
server 10.2.2.2
server 10.3.3.3
```

aaa netconf-accounting

To enable authentication, authorization, and accounting (AAA) accounting of netconf services for billing or security purposes when you use TACACS+, use the **aaa netconf-accounting** command in global configuration mode or template configuration mode. To disable AAA accounting, use the **no** form of this command.

aaa netconf-accounting

aaa netconf-accounting { **system** | **exec** | **network** | **connection** *connection-name* }

Syntax Description

system	Performs accounting for all system-level events not associated with users, such as reloads. **Note** When system accounting is used and the accounting server is unreachable at system startup time, the system will not be accessible for approximately two minutes.
exec	Runs accounting for the EXEC shell session. This keyword might return user profile information such as what is generated by the **autocommand** command.
network	Runs accounting for all network-related service requests.
connection	Provides information about all outbound connections made from the network access server, such as Telnet, local-area transport (LAT), TN3270, packet assembler and disassembler (PAD), and rlogin.

Command Default

AAA accounting is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco Catalyst SD-WAN Manager Release 20.15.1	Command is introduced.

Usage Guidelines

The **system aaa netconf-accounting** configuration depends on **system aaa accounting**. Only when **system aaa netconf-accounting** is configured, the netconf-accouting also can be configured.

When **system aaa accounting** is deleted, **system aaa netconf-accounting** is also deleted. However, when you delete **system aaa netconf-accounting**, there is no effect on **system aaa accounting**.

Example

The following example shows how to configure netconf accounting:

```
Device (config)# system
Device (config)# aaa netconf-accounting aaalist1
Device (config)#
```

ip tacacs source-interface

To use the IP address of a specified interface for all outgoing TACACS+ packets, use the **ip tacacs source-interface** command in global configuration mode. To disable use of the specified interface ip address, use the **no** form of this command.

ip tacacs source-interface *interface-name*
no ip tacacs source-interface *interface-name*

Syntax Description

interface-name	Name of the interface that TACACS+ uses for all its outgoing packets.

Command Default

None

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines Use **ip tacacs source-interface** command to set the IP address of a subinterface for all outgoing TACACS+ packets. This address is used if the interface is in the up state. In this way, the TACACS+ server can use one IP address entry associated with the network access client instead of maintaining a list of all IP addresses. You can use the **ip tacacs source-interface** command when the router has many interfaces and ensure that all TACACS+ packets from a particular router have the same IP address. The specified interface must have an IP address associated with it. If the specified subinterface does not have an IP address or is in a down state, TACACS+ reverts to the default. To avoid this, add an IP address to the subinterface or bring the interface to the up state.

Example

The following example configures TACACS+ to use the IP address of the loopback0 interface for all outgoing TACACS+ packets.

```
Device(config)# ip tacacs source-interface loopback0
```

ip vrf forwarding (server-group)

To associate a Virtual Private Network (VPN) routing and forwarding (VRF) reference of an authentication, authorization, and accounting (AAA) TACACS+ server group, use the **ip vrf forwarding** command in server-group configuration mode. To enable server groups to use the global (default) routing table, use the no form of this command.

ip vrf forwarding *vrf-name*
no ip vrf forwarding *vrf-name*

Syntax Description

name	Name assigned to a VRF.

Command Default Server groups use the global routing table.

Command Modes

Server-group configuration (server-group)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1r	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

Use the **ip vrf forwarding** command to specify a VRF for a AAA TACACS+ server group. This command enables dial users to utilize AAA servers in different routing domains.

Examples

The following example shows how to configure the VRF user using a AAA

```
aaa group server tacacs+ tacacs-511
server-private 172.16.0.1 key 7 110a1016141d
ip vrf forwarding 511
```

lockout-policy

To configure Cisco SD-WAN Manager and other controllers to lock out users who have made a designated number of consecutive unsuccessful login attempts within a designated period, or who have not logged in for a designated number of days, use the **lockout-policy** command in global configuration mode. To disable the lockout policy, use the **no** form of this command.

lockout-policy {[fail-attempts *attempts* **fail-interval** *fail-interval* [**lockout-interval** *lockout-interval*]] [**num-inactive-days** *days*]}

no lockout-policy {[fail-attempts *attempts* **fail-interval** *fail-interval* [**lockout-interval** *lockout-interval*]] [**num-inactive-days** *days*]}

Syntax Description

fail-attempts *attempts*	Specifies the number of consecutive times a user unsuccessfully attempts to log in to Cisco SD-WAN Manager or other controllers after which the user is locked out. **Note** Attempting to log in through the CLI without providing a password is counted as a failed login attempt. Default: 5 Range: 1 through 3600
fail-interval *fail-interval*	Specifies the period, in seconds, in which consecutive unsuccessful login attempts are counted. For example, if this period is set to 10 seconds and the number of failed login attempts is set to 5, a user is locked out if the user makes 5 consecutive unsuccessful login attempts within 10 seconds. Default: 900 Range: 1 through 3600

lockout-interval *lockout-interval*	Specifies the period, in seconds, after which a user who is locked out because of unsuccessful login attempts can log in. If you do not configure this period, an administrator must manually unlock the account of a locked-out user. Default: 900 Range: 0 through 3600
num-inactive-days *days*	Specifies the number of days since a user last logged in to Cisco SD-WAN Manager or other controllers after which the user is locked out. Range: 2 through 365

Command Default

This command is disabled, and so a lockout policy is not in effect. In this case, by default, Cisco SD-WAN Manager and other controllers allow five consecutive unsuccessful password attempts before an account is locked for 15 minutes or until an administrator unlocks it.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 17.12.1a	This command was introduced.

Usage Guidelines

When you configure a lockout policy, users who violate the policy cannot log in again until a configured amount of time has passed or an administrator unlocks their accounts in Cisco SD-WAN Manager and other controllers.

Examples

The following example shows how to configure a lockout policy of three failed login attempts over a period of 300 seconds, and a reset period of 100 seconds:

```
device(config-system)# aaa
device (config-aaa)# lockout-policy
device (config-lockout-policy)# fail-attempts 3 fail-interval 300 lockout-interval 100
```

The following example shows how to configure an inactivity lockout period of 30 days for user logins:

```
device(config-system)# aaa
device (config-aaa)# lockout-policy
device (config-lockout-policy)# num-inactive-days 30
```

Related Commands

Command	Description
aaa authentication attempts login	Sets the maximum number of login attempts that are permitted before a session is dropped.

Command	Description
multi-factor-auth duo	Configures controllers to require Duo multifactor authentication (MFA) to verify the identity of users before they can log in.

login block-for

To configure your Cisco IOS device for login parameters that help provide denial-of-service (DoS) detection, use the **login block-for**command in global configuration mode. To disable the specified login parameters and return to the default functionality, use the **no** form of this command.

login block-for *seconds* **attempts** *tries* **within** *seconds*
no login block-for

Syntax Description

seconds	Duration of time in which login attempts are denied (also known as a quiet period) by the Cisco IOS device. Valid values range from 1 to 65535 (18 hours) seconds.
attempts *tries*	Maximum number of failed login attempts that triggers the quiet period. Valid values range from 1 to 65535 tries.
within *seconds*	Duration of time in which the allowed number of failed login attempts must be made before the quiet period is triggered. Valid values range from 1 to 65535 (18 hours) seconds.

Command Default

No login parameters are defined.

A quiet period is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 17.3.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE login block-for command.

Examples

The following example shows how to configure your router to block all login requests for 100 seconds if 15 failed login attempts are exceeded within 100 seconds. Thereafter, the **show login** command is issued to verify the login settings.

```
Device(config)# login block-for 100 attempts 15 within 100
Device(config)# exit
Device# show login
A default login delay of 1 seconds is applied.
No Quiet-Mode access list has been configured.
All successful login is logged.
All failed login is logged.
Router enabled to watch for login Attacks.
If more than 15 login failures occur in 100 seconds or less, logins will be disabled for
100 seconds.
```

```
Router presently in Watch-Mode, will remain in Watch-Mode for 95 seconds.
Present login failure count 5
```

The following example shows how to disable login parameters. Thereafter, the **show login** command is issued to verify that login parameters are no longer configured.

```
Router(config)# no login block-for
Router(config)# exit
Router# show login
No login delay has been applied.

     No Quiet-Mode access list has been configured.

     All successful login is logged.


     Router NOT enabled to watch for login Attacks
```

login quiet-mode access-class

To specify an access control list (ACL) that is to be applied to the router when the router switches to quiet mode, use the **login quiet-mode access-class**command in global configuration mode. To remove this ACL and allow the router to deny all login attempts, use the **no** form of this command.

login quiet-mode access-class {*acl-nameacl-number*}
no login quiet-mode access-class {*acl-nameacl-number*}

Syntax Description

acl-name	Named ACL that is to be enforced during quiet mode.
acl-number	Numbered (standard or extended) ACL that is to be enforced during quiet mode.

Command Default

All login attempts via Telnet, secure shell (SSH), and HTTP are denied.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 17.3.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE login quiet-mode access-class command.

Quiet-mode does not support **vrf-also** command. When the router is on quiet mode, the ACL restricts the access to the device. This feature works only when you try to access the device through transport or a non-vrf interface.

Examples

The following example shows how to configure your router to accept hosts only from the ACL "myacl" during the next quiet period:

```
Device(config)# login quiet-mode access-class myacl
```

login-rate

To configure a threshold for detecting frequent logins, use the **login-rate** command in alarms configuration mode.

Use the **no** form of the command to clear the configuration.

Cisco SD-WAN Manager

login-rate { **interval** *seconds* | **num-logins** *count* }

no login-rate

Syntax Description

interval *seconds*	Specify the interval in seconds.
num-logins *count*	Specify the number of logins to be reached before generating an alarm.

Command Modes

Alarms configuration (config-alarms)

Command History

Release	Modification
Cisco Catalyst SD-WAN Control Components Release 20.12.1	This command was introduced.

Examples

The following example shows how to configure the login-rate alarm parameters:

```
sdwan-manager(config)# system
sdwan-manager(config-system)# alarms
sdwan-manager(config-alarms)# login-rate interval 60 num-logins 3
```

Related Commands

Command	Description
alarms	Configures CPU-usage watermarks and polling interval.
show alarms	Displays alarm history and watermarks for CPU, memory, and disk usage, and the disk read and write speeds.

multi-factor-auth duo

To configure Cisco SD-WAN Manager and other controllers to require Duo multifactor authentication (MFA) to verify the identity of users before they can log in, use the multi-factor-auth duo command in global configuration mode. To disable Duo MFA authentication for controllers, use the no form of this command.

multi-factor-auth duo api-hostname *name* **integration-key** *i-key* **secret-key** *s-key*
proxy *proxy-url*

no multi-factor-auth duo api-hostname *name* **integration-key** *i-key* **secret-key** *s-key*

proxy *proxy-url*

Syntax Description

api-hostname *name*	Specifies the API hostname (api-hostname) of your Duo account.
integration-key *i-key*	Specifies the integration key (Ikey) of your Duo account.
secret-key *s-key*	Specifies the secret key (Skey) of your Duo account.
proxy *proxy-url*	Specifies the URL of the proxy that is used to access the Duo server if Cisco SD-WAN Manager is behind a firewall. If an HTTP proxy is configured for Cisco SD-WAN Manager, this proxy is the default value.

Command Default

This command is disabled. So, Cisco SD-WAN Manager and other controllers do not require Duo MFA to verify the identity of users before they log in.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 17.12.1a	This command was introduced.

Usage Guidelines

- You must have a Duo account with local users created on that account.
- When you configure this command, users are prompted on their mobile devices to authenticate with Duo after they enter a username and password to log in to Cisco SD-WAN Manager or other controllers.
- Duo MFA does not apply to the admin user by default. If you want to enable Duo MFA for the admin user, configure multi-factor-auth duo, then enter the admin-auth-order command.
- If Cisco SD-WAN Manager or another controller does not have internet access, use the following commands to configure proxy information for the device on which Duo MFA is enabled. Enter these commands either from the command line of the device or its device template. This configuration provides access to the Duo MFA feature. The device can be a Cisco SD-WAN Manager server, a Cisco Catalyst SD-WAN Validator, or a Cisco Catalyst SD-WAN Controller.

```
vm # config
vm(config)# system aaa
vm(config-aaa)# multi-factor-auth
vm(config-multi-factor-auth)# duo
vm(config-duo)# api-hostname name
vm(config-duo)# secret-key s-key
vm(config-duo)# integration-key i-key
vm(config-duo)# proxy proxy-url
vm(config-duo)# commit
```

Examples

The following example shows how to configure Cisco SD-WAN Manager and other controllers to require Duo MFA to verify the identity of users before they can log in:

```
device(config-system)# aaa
device (config-aaa)# multi-factor-auth duo
device (config-duo)# api-hostname api-xxxxxxxx.duosecurity.com
device (config-duo)# integration-key DIMVTNxxxxxxxxxx
device (config-duo)# secret-key Mxxxxxxxxxxxxx
```

Related Commands

Command	Description
aaa authentication attempts login	Sets the maximum number of login attempts that are permitted before a session is dropped.
lockout-policy	Configures Cisco SD-WAN Manager and other controllers to lock out users who have made a designated number of consecutive unsuccessful login attempts within a designated period, or who have not logged in for a designated number of days.

server-private (TACACS+)

To configure the IPv4 or IPv6 address of the private TACACS+ server for the group server, use the **server-private** command in TACACS+ 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* [**port** *port-number* | **timeout** *interval* | **key** [**0** | **6** | **7**] *key-string*]

no server-private *ip-address* [**port** *port-number* | **timeout** *interval* | **key** [**0** | **6** | **7**] *key-string*]

Syntax Description

ip-address	IP address of the private RADIUS or TACACS+ server host.
port *port-number*	(Optional) Specifies the server port number. This option overrides the default, which is port 49. Range: 1 to 65535
timeout *interval*	(Optional) Specifies the server timeout interval. Range: 1 to 1000
key [**0** | **6** | **7**]	(Optional) Specifies an authentication and encryption key. This key must match the key used by the TACACS+ daemon. Specifying this key overrides the key set by the global**tacacs-server key** command for this server only. • If no number or 0 is entered, the string that is entered is considered to be plain text. If 6 is entered, the string that is entered is considered to be an advanced encryption scheme [AES] encrypted text. If 7 is entered, the string that is entered is considered to be hidden text.
key-string	(Optional) Character string specifying the authentication and encryption key.

Command Default

If server-private parameters are not specified, global configurations are used; if global configurations are not specified, default values are used.

Command Modes TACACS+ server-group configuration (config-sg-tacacs+)

Command History

Release	Modification
Cisco IOS XE SD-WAN Release 17.2.1r	Command qualified for use in Cisco vManage CLI templates.
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	**Port** and **Timeout** keywords added in AAA named server implementation.

Usage Guidelines For usage guidelines, see the Cisco IOS XE server-private (TACACS+) command.

Examples

The following example shows how to define the TACACS+ group server and associate private servers with it:

```
Device> enable
Device# config-transaction
Device(config)# aaa group server tacacs+ tacacs1
Device(config-sg-tacacs+)# server-private 172.16.0.1 key 7 110a1016141d
```

The following example shows how to configure TACACS+ group server port number and timeout interval:

```
Device(config)# aaa group server tacacs+ tacacs1
Device(config-sg-tacacs+)# server-private 172.16.0.1 port 49 timeout 100
```

tacacs server address ipv4

To set the IPv4 address of a specified TACACS+ server, use the **tacacs server address ipv4** command in global configuration mode. To remove the IPv4 address associated with the specified TACACS+ server, use the **no** form of this command.

tacacs server *server-name* **address ipv4** *ipv4-address*
no tacacs server *server-name* **address ipv4** *ipv4-address*

Syntax Description

server-name	Name of TACACS+ server.
ipv4-address	TACACS+ server IPv4 address in the A.B.C.D format.

Command Default None

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines Use **tacacs server address ipv4** command to set an IP address for a known TACACS+ server.

Example

The following example configures an IP address of 10.10.10.10 for the TACACS+ server "tacacsserver".

```
Device(config)# tacacs server tacacsserver address ipv4 10.10.10.10
```

tacacs server key

To set an authentication and encryption key of a specified TACACS+ server, use the **tacacs server key** command in global configuration mode. To remove the key associated with the specified TACACS+ server, use the **no** form of this command.

tacacs server *server-name* **key** [*key*]
no tacacs server *server-name* **key** [*key*]

Syntax Description

server-name	Name of TACACS+ server.
key	(optional) Specifies an authentication and encryption key. This must match the key used by the TACACS+ daemon.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Use **tacacs server key** command to set an authentication and encryption key for a known TACACS+ server.

Example

The following example configures an authentication and encryption key "Ys6WhgHS40" for the TACACS+ server "tacacsserver".

```
Device(config)# tacacs server tacacsserver key Ys6WhgHS40
```

tacacs server port

To set the port on which the TACACS server connects with the server host, use the **tacacs server port** command in global configuration mode. To reset port settings, use the **no** form of this command.

tacacs server *server-name* **port** *port-number*
no tacacs server *server-name* **port** *port-number*

Syntax Description

port-number	Specifies the port number. The range is from 1 to 65535. The default value is 49.
server-name	Specifies the name of the private TACACS+ server host.

Command Default

The default port on which the server connects with the server host is 49.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	This command was introduced.

Usage Guidelines

Use the port integer argument to specify the TCP port number to be used when making connections to the TACACS+ daemon. The default port number is 49.

Examples

The following example shows how to configure the port to 49:

```
Device(config)# tacacs server server1
Device(config-server-tacacs)# timeout 20

Device(config)# tacacs server server1
Device(config-server-tacacs)# port 49
```

tacacs server timeout

To set the interval for which the TACACS server waits for a server host to reply, use the **tacacs server timeout** command in global configuration mode. To restore the default timeout interval, use the **no** form of this command.

tacacs server *name* **timeout** *seconds*
no tacacs server *name* **timeout**

Syntax Description

name	Name of the private TACACS+ server host.
timeout	Configures the time to wait for a reply from the specified TACACS server.
seconds	Timeout interval, in seconds. The range is from 1 to 1000. The default is 5.

Command Default

The default timeout interval for which the server waits for the server host to reply is 5 seconds.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE tacacs server timeout command.

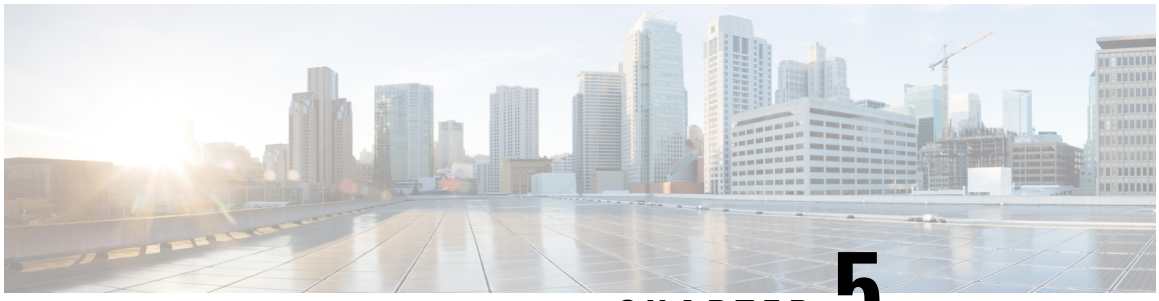
Examples

The following example shows how to set the timeout interval to 20 seconds:

```
Device(config)# tacacs server server1 timeout 20
```

Related Commands

Command	Description
tacacs-server host	Specifies a TACACS+ host.
tacacs server address ipv4	Sets the IPv4 address of a specified TACACS+ server.
tacacs server key	Sets an authentication and encryption key of a specified TACACS+ server.



CHAPTER 5

ACL Commands

- deny, on page 35
- ip access-list, on page 38
- ipv6 access-list, on page 39
- permit, on page 39
- sequence, on page 42

deny

To set conditions in a named IP access list or object group access control list (OGACL) that will deny packets, use the **deny** configuration command in the appropriate configuration mode. To remove a deny condition from an IP access list or OGACL, use the **no** form of this command.

TCP or UDP

sequence-number **deny** { *tcp* | *udp* } { *src-addr* *src-wildcard* | **any** | **host** *addr* | **object-group** *src-network-group* } [**eq** *port* | **range** *min-port* *max-port*] { *dest-addr* *dest-wildcard* | **any** | **host** *addr* | **object-group** *dest-network-group* } [**eq** *port* | **range** *min-port* *max-port*] [**log**]
no *sequence-number* [**deny**] [| { *tcp* | *udp* } | { *src-addr* *src-wildcard* | **any** | **host** *addr* | **object-group** *src-network-group* } | [**eq** *port* | **range** *min-port* *max-port*] | { *dest-addr* *dest-wildcard* | **any** | **host** *addr* | **object-group** *dest-network-group* } | [**eq** *port* | **range** *min-port* *max-port*]] [**log**]

All other protocols

sequence-number **deny** { *protocol* | **object-group** *service-group* } { *src-addr* *src-wildcard* | **any** | **host** *addr* | **object-group** *src-network-group* } { *dest-addr* *dest-wildcard* | **any** | **host** *addr* | **object-group** *dest-network-group* } [**log**]

no *sequence-number* [**deny**] [{ *protocol* | **object-group** *service-group* } | { *src-addr* *src-wildcard* | **any** | **host** *addr* | **object-group** *src-network-group* } | { *dest-addr* *dest-wildcard* | **any** | **host** *addr* | **object-group** *dest-network-group* | **range** *port* } | [**log**]]

Syntax Description

sequence-number	Specify a sequence number to **permit** or **deny** statements to order the statement in the list . You also can use sequence numbers to reorder, add, or remove statements in a list.

protocol	Name or number of a protocol; valid values are **eigrp**, **gre**, **icmp**, **igmp**, **igrp**, **ip**, **ipinip**, **nos**, **ospf**, **tcp**, or **udp**, or an integer in the range 0 to 255 representing an IP protocol number. To match any Internet protocol (including Internet Control Message Protocol (ICMP), TCP, and User Datagram Protocol (UDP), use the keyword **ip**. See the "Usage Guidelines" section for additional qualifiers.
object-group*service-group*	Specify an object group of type **service**.
src-addr	Number of the source network or host from which the packet is being sent in a 32-bit quantity in four-part, dotted-decimal format.
src-wildcard	Wildcard bits to be applied to source network in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore.
any	Specifies any source or any destination host as an abbreviation for the *source-addr*or *destination-addr value*and the *source-wildcard* or *destination-wildcard* value of 0.0.0.0 255.255.255.255.
host *addr*	Specifies the source or destination address of a single host.
tcp	Specifies the TCP protocol.
udp	Specifies the UDP protocol.
object-group *source-addr-group-name*	Specifies the name of the object-group that contains the group of source addresses. The source and destination object groups must be **network** object groups. You cannot use empty object groups in access control lists.
destination-addr	Number of the network or host to which the packet is being sent in a 32-bit quantity in four-part, dotted-decimal format.
destination-wildcard	Wildcard bits to be applied to the destination in a 32-bit quantity in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore.
object-group *dest-addr-group-name*	Specifies the name of the object-group that contains the group of destination addresses. The source and destination object groups must be **network** object groups. You cannot use empty object groups in access control lists.

log	(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the **logging console** command.) The message for a standard list includes the access list number, whether the packet was permitted or denied, the source address, and the number of packets. The message for an extended list includes the access list number; whether the packet was permitted or denied; the protocol; whether the protocol was TCP, UDP, ICMP, or a number; and, if appropriate, the source and destination addresses and source and destination port numbers. For both standard and extended lists, the message is generated for the first packet that matches, and then at 5-minute intervals, including the number of packets permitted or denied in the prior 5-minute interval. The logging facility might drop some logging message packets if there are too many to be handled or if there is more than one logging message to be handled in 1 second. This behavior prevents the router from reloading because of too many logging packets. Therefore, the logging facility should not be used as a billing tool or an accurate source of the number of matches to an access list.

Command Default

There is no specific condition under which a packet is denied passing the access list.

Command Modes

Standard access-list configuration (config-std-nacl)
Extended access-list configuration (config-ext-nacl)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Additional parameters qualified: `udp`, `tcp`, `icmp`, and `range`

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `deny` command.

Examples

```
ip access-list standard 10
 10 deny 10.1.1.1

ip access-list standard 15
 10 deny any

ip access-list extended 105
 10 deny ip any any

ip access-list extended 105
 10 deny ip host 10.1.1.1 any
 20 deny object-group OBJ_PROTO object-group OBJ_SRC object-group OBJ_DEST

ip access-list extended EXTACL
 10 deny ip any any log
```

ip access-list

To define an IP access list or object-group access control list (ACL) by name or number or to enable filtering for packets with IP helper-address destinations, use the **ip access-list** command in global configuration mode. To remove the IP access list or object-group ACL or to disable filtering for packets with IP helper-address destinations, use the **no** form of this command.

ip access-list { { **standard** | **extended** } { *access-list-name access-list-number* } }
no ip access-list { { **standard** | **extended** } { *access-list-name access-list-number* } }

Syntax Description

standard	Specifies a standard IP access list. You can only filter based on the source with standard IP access lists.
extended	Specifies an extended IP access list. Required for object-group ACLs.
access-list-name	Name of the IP access list or object-group ACL. Names cannot contain a space or quotation mark, and must begin with an alphabetic character to prevent ambiguity with numbered access lists.
access-list-number	Number of the access list. • A standard IP access list is in the ranges 1-99 or 1300-1999. • An extended IP access list is in the ranges 100-199 or 2000-2699.

Command Default

No IP access list or object-group ACL is defined, and outbound ACLs do not match and filter IP helper relayed traffic.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	`ip access-list extended` command qualified for use in Cisco vManage CLI templates.
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Additional parameter qualified: `ip access-list standard`

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `ip access-list` command.

Examples

```
ip access-list standard 10
 10 deny 10.1.1.1
```

```
ip access-list standard 15
 10 deny any
```

```
ip access-list standard 15
 10 deny ip-address
```

```
ip access-list extended 105
 10 deny ip 10.1.1.1 any
 20 deny ip object-group1 any
```

In the following example, the source IP address is 10.1.1.1 and the destination IP address is 10.1.1.2

```
ip access-list extended 105
  10 permit host 10.1.1.1 10.1.1.2
```

```
ip access-list extended 105
 10 deny ip any any
```

```
ip access-list extended EXTACL
 10 deny ip any any log
```

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.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE ipv6 access-list command.

Examples

```
Device# config-transaction
Device(config)# ipv6 access-list test300_v6
Device(config-ip-acl)# sequence 100 permit ipv6 any 2001:DB8::/32
Device(config-ip-acl)#
```

permit

To set conditions in named IP access list that will permit packets, use the **permit** command in the appropriate configuration mode. To remove a condition from an IP access list, use the **no** form of this command.

Syntax Description

sequence-number	Specify a sequence number to **permit** or **deny** statements to position the statement in the list. You can also use sequence numbers to reorder, add, or remove statements in a list.
protocol	Name or number of a protocol; valid values are; valid values are **ahp**, **eigrp**, **esp**, **gre**, **icmp**, **igmp**, **igrp**, **ip**, **ipinip**, **nos**, **ospf**, , **tcp**, **pcp**, **pim**, **udp**, or an integer in the range 0 to 255 representing an IP protocol number. To match any Internet protocol (including Internet Control Message Protocol (ICMP), TCP, and User Datagram Protocol (UDP), use the keyword **ip**. See the “Usage Guidelines” section for additional qualifiers.
object-group*service-group*	Specify an object group of type **service**.

source-addr	(Optional) Number of the network or host from which the packet is being sent in a 32-bit quantity in four-part, dotted-decimal format.
source-wildcard	(Optional) Wildcard bits to be applied to the source in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore.
any	Specifies any source or any destination host as an abbreviation for the *source-addr*or *destination-addr value*and the *source-wildcard* or *destination-wildcard* value of 0.0.0.0 255.255.255.255.
host *address name*	Specifies the source or destination address and name of a single host.
object-group *source-addr-group-name*	Specifies the name of the object group that contains the group of source addresses. The source and destination object groups must be **network** object groups. You cannot use empty object groups in access control lists.
destination-addr	Number of the network or host to which the packet is being sent in a 32-bit quantity in four-part, dotted-decimal format.
destination-wildcard	Wildcard bits to be applied to the destination in a 32-bit quantity in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore.
object-group *dest-addr-group-name*	Specifies the name of the object-group that contains the group of destination addresses. The source and destination object groups must be **network** object groups. You cannot use empty object groups in access control lists.
log	(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the **logging console** command.) The message for a standard list includes the access list number, whether the packet was permitted or denied, the source address, and the number of packets. The message for an extended list includes the access list number; whether the packet was permitted or denied; the protocol; whether the protocol was TCP, UDP, ICMP, or a number; and, if appropriate, the source and destination addresses and port numbers and the user-defined cookie or router-generated hash value. For both standard and extended lists, the message is generated for the first packet that matches, and then at 5-minute intervals, including the number of packets permitted or denied in the prior 5-minute interval. The logging facility might drop some logging message packets if there are too many to be handled or if there is more than one logging message to be handled in 1 second. This behavior prevents the router from reloading because of too many logging packets. Therefore, the logging facility should not be used as a billing tool or an accurate source of the number of matches to an access list. After you specify the **log** keyword (and the associated *word* argument), you cannot specify any other keywords or settings for this command.
tcp	Specifies the TCP protocol.
udp	Specifies the UDP protocol.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Additional parameters qualified: `udp`, `tcp`, `icmp`, and `range`
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Additional parameters qualified: `geo-group`

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `permit` command.



Note You can configure a fully qualified domain name (FQDN) or a GEO as a source object group or as a destination object group using an Access Control List (ACL). Do not configure both a GEO and an FQDN as a source or destination object group.

```
object-group fqdn asdfa-Rule_2-fqdn-src_
pattern "www\.cisco\.com"
!
object-group fqdn asdfa-Rule_4-fqdn-dstn_
pattern "www\.cnn\.com"
!
object-group geo asdfa-Rule_1-geo-src_
country AGO
!
object-group geo asdfa-Rule_3-geo-dstn_
country CMR
!
object-group service asdfa-Rule_1-svc_
ip
!
object-group service asdfa-Rule_2-svc_
ip
!
object-group service asdfa-Rule_3-svc_
ip
!
object-group service asdfa-Rule_4-svc_
ip

ip access-list extended asdfa-seq-Rule_1-acl_
19 permit object-group asdfa-Rule_1-svc_ geo-group asdfa-Rule_1-geo-src_ any
!
ip access-list extended asdfa-seq-Rule_2-acl_
14 permit object-group asdfa-Rule_2-svc_ fqdn-group asdfa-Rule_2-fqdn-src_ any
!
ip access-list extended asdfa-seq-Rule_3-acl_
15 permit object-group asdfa-Rule_3-svc_ any geo-group asdfa-Rule_3-geo-dstn_
!
ip access-list extended asdfa-seq-Rule_4-acl_
12 permit object-group asdfa-Rule_4-svc_ any fqdn-group asdfa-Rule_4-fqdn-dstn_
```

sequence

To specify a sequence number for the permit condition in the IP access list, use the **sequence** command in the appropriate configuration mode. To remove a sequence number from an IP access list, use the **no** form of this command.

sequence *sequence-number* { **permit** } { **ipv6** } { **any** *ipv6-address* }

Syntax Description

sequence-number	Permits statements to position the statement in the list.
permit	Sets permit conditions for an IPv6 access list.
ipv6	Sets the IPv6 address to set permit conditions.
any *ipv6-address*	Specifies any source or any destination host as an abbreviation for the *source-addr* or *destination-addr value* and the *source-wildcard* or *destination-wildcard* value of 0.0.0. 255.255.255.255.

Command Default

There are no specific conditions under which a packet passes the access list.

Command Modes

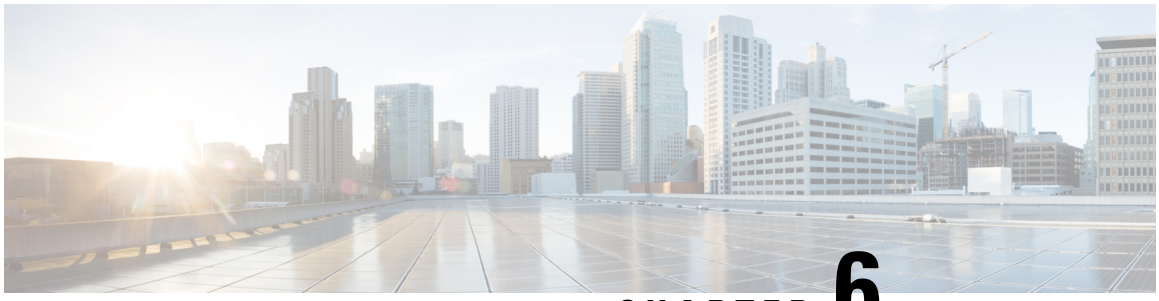
IPv6 access-list configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

Examples

```
Device(config)# ipv6 access-list test300_v6
Device(config-ipv6-acl)# sequence 100 permit ipv6 any 2001:DB8::/32
```



CHAPTER 6

AppNav Commands

- appnav-controller, on page 43
- service-insertion, on page 44
- service-insertion appnav-controller-group, on page 45
- service-node-group, on page 46
- service-insertion waas interface, on page 47
- service node, on page 47
- service-policy, on page 48

appnav-controller

To configure IPv4 addresses for an AppNav Controller, use **appnav-controller** command in Service Insertion AppNav Controller-group configuration mode. To remove the AppNav controller, use the **no** form of this command.

appnav-controller *ipv4address* **vrf** *vrf*
no appnav-controller *ipv4address* **vrf** *vrf*

Syntax Description

ipv4address	Specifies the IPv4 address of the AppNav controller.
vrf	Specifies the service VRF.

Command Default

None

Command Modes

Service insertion AppNav controller-group configuration (config-service-insertion-acg).

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	This command was introduced.

Usage Guidelines

The AppNav-XE component is made up of a distribution unit called the AppNav controller and service nodes. The AppNav controller intercepts network traffic and based on an AppNav policy, distributes that traffic to one or more WAAS nodes for optimization. The device in this context is a Cisco WAN edge device running AppNav-XE.

The AppNav Controller group configures the AppNav Controller. To configure the AppNav Controller group, enter the IP addresses used by the AppNav Controllers.

Examples

The following example shows how to configure the IP address 192.3.3.1 as an AppNav controller for traffic interception on VRF 2.

```
Device(config)# service-insertion appnav-controller-group scg
Device(config-service-insertion-acg)# appnav-controller 192.3.3.1 vrf 2
```

Table 6: Related Commands

Command	Description
service-insertion appnav-controller-group	Configures an AppNav Controller Group.

service-insertion

To configure an AppNav Controller group (ANCG), Service Node Group (SNG) and service context that is part of an AppNav Cluster, use the **service-insertion** command. To unconfigure settings, use the no form of this command.

service-insertion { **appnav-controller-group** *ancgroupname* | **service-node-group** *sngroupname* | **service-context** *contextname* { **waas** } | **waas interface** *interface* }

no service-insertion

Syntax Description

ancgroupname	Specifies the name of an ANCG to configure and enters AppNav Controller group configuration mode to configure ANCG settings. If the ANCG does not exist, this command creates it.
sngroupname	Specifies the name of a SNG to configure and enters service node group configuration mode to configure SNG settings. If the SNG does not exist, this command creates it.
contextname	Specifies the service context name to configure and enters service context group configuration mode to configure service context settings. If the service context does not exist, this command creates it.

Command Default

No default behavior or values.

Command Modes

global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines Use this command to create service controller group, service node group and service insertion context.

Examples The following is an example of this command:

```
service-insertion appnav-controller-group scg
  appnav-controller 192.3.3.1 vrf 2
  appnav-controller 192.3.3.2 vrf 2
 !
 service-insertion service-node-group acg1
  service-node 192.3.3.3
 !
 service-insertion service-context waas/1
  appnav-controller-group scg
  service-node-group      acg1
  service-policy          p1
  enable
 !
 service-insertion waas interface Tunnel2
 service-insertion waas interface Tunnel3
 !
```

service-insertion appnav-controller-group

To configure an AppNav controller group, use **service-insertion appnav-controller-group** command in global configuration mode. To remove the AppNav controller group, use the **no** form of this command.

service-insertion appnav-controller-group *group-name*
no service-insertion appnav-controller-group *group-name*

Syntax Description

group-name	Specifies the name of the AppNav controller group.

Command Default None

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	This command was introduced.

Usage Guidelines The AppNav-XE component is made up of a distribution unit called the AppNav controller and service nodes. The AppNav Controller intercepts network traffic and based on an AppNav policy, distributes that traffic to one or more WAAS nodes for optimization. The device in this context is a Cisco Catalyst SD-WAN edge device running AppNav-XE.

Use the **service-insertion appnav-controller-group** command to configure an AppNav controller group. You can configure different AppNav controllers on the AppNav controller group.

Examples

The following example shows how to configure the IP address 192.3.3.1 as an AppNav controller for traffic interception on VRF 2 on the AppNav controller group scg.

```
Device# config-transaction
Device(config)# service-insertion appnav-controller-group scg
Device(config-service-insertion-acg)# appnav-controller 192.3.3.1 vrf 2
```

Table 7: Related Commands

Command	Description
appnav-controller	Configures an AppNav controller.

service-node-group

To configure the name of a SNG to be used in a service context, use the **service-node-group** service context configuration command. To unconfigure the SNG, use the no form of this command.

service-node-group *sngroupname*

no service-node-group *sngroupname*

Syntax Description

service-node-group*sngroupname*	Specifies the name of a SNG to add to the service context. The SNG must have been previously configured by the **service-insertion service-node-group** command.

Command Default

No default behavior or values.

Command Modes

Service context configuration (config-service-insertion-context)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

An AppNav Cluster can have up to 32 member SNGs and a maximum of 32 service nodes.

Examples

The following example shows how to configure this command:

```
service-insertion service-context waas/1
  service-node-group      acg1
```

service-insertion waas interface

To enable WAAS service AppNav interception for an interface, use the **service-insertion waas interface** command in global configuration mode. To disable WAAS service AppNav interception for an interface, use the **no** form of this command.

service-insertion waas interface *interface*
no service-insertion waas interface *interface*

Syntax Description

interface	Specifies the name of the interface for WAAS service AppNav interception.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	This command was introduced.

Usage Guidelines

The AppNav-XE component is made up of a distribution unit called the AppNav controller and service nodes. The AppNav controller intercepts network traffic and, based on an AppNav policy, distributes that traffic to one or more WAAS nodes for optimization. The device in this context is a Cisco Catalyst SD-WAN edge device running AppNav-XE.

Use **service-insertion waas interface** command to enable WAAS service AppNav interception for an WAN interface, and in the case of a Cisco Catalyst SD-WAN Overlay, a tunnel interface on the transport side (VPN 0).

Examples

The following example shows how to WAAS service AppNav interception for interfaces tunnel 2 and tunnel 3, both transport interfaces for a WAN edge device.

```
Device(config)# service-insertion waas interface Tunnel2
Device(config)# service-insertion waas interface Tunnel3
```

service node

To configure the IP address to be added to the SNG, use the **service-node** service node group configuration command. To unconfigure the IP address, use the **no** form of this command.

service-node *ip-address*

no service-node *ip-address*

Syntax Description

ip-address	Specifies the IP address of a service node to be added to the SNG. The address must be the IP address of the interface on which the service node is to receive traffic.

Command Default

No default behavior or values.

Command Modes

Service node group configuration (config-service-insertion-sng)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

Use this command to create service node.

Examples

The following example shows how to configure the IP address of a service node:

```
device(config)# service-insertion service-node-group acg1
device(config-service-insertion-sng)# service-node 10.10.10.15
```

service-policy

To configure AppNav and optimization service policy, use the **service-policy** global configuration command. To unconfigure settings, use the no form of this command

service-policy *policyname*

no service-policy *policyname*

Command Default

None.

Command Modes

Service context configuration (config-service-insertion-context)

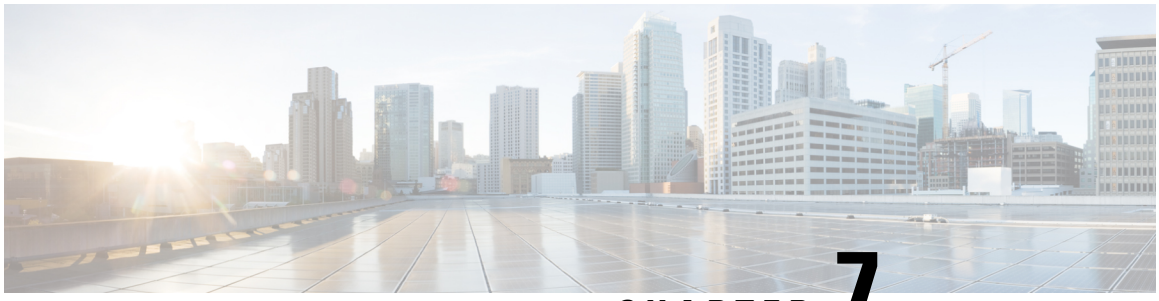
Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Examples

```
service-insertion service-context waas/1
  service-policy          p1


class test101-seq-21-cm_
  service-policy avc Yahoo-pm_
```



CHAPTER 7

AppQoE Commands

- (config-scxt) appnav-controller-group , on page 49
- app-resource package-profile, on page 50
- appqoe http-connect, on page 51
- appqoe tcpopt enable, on page 51
- app-hosting, on page 52
- app-hosting appid, on page 53
- app-vnic, on page 54
- cluster-type, on page 55
- device-role, on page 55
- dreopt enable, on page 56
- dual-side optimization enable, on page 56
- exporter, on page 57
- guest-ipaddress, on page 58
- iox, on page 59
- performance monitor apply, on page 59
- performance monitor context, on page 60
- performance monitor sampling-rate, on page 61
- platform resource, on page 62
- rd, on page 63
- sdwan appqoe dreopt enable, on page 63
- service-insertion appqoe, on page 64
- service-insertion appnav-controller-group appqoe, on page 64
- **service-insertion service-node-group** appqoe, on page 66
- start (app-hosting), on page 66
- traffic-monitor, on page 67
- vrf (service-insertion-context), on page 68

(config-scxt) appnav-controller-group

To configure the name of the ANCG to be used in a service context, use the **appnav-controller-group** service context configuration command. To unconfigure the ANCG, use the **no** form of this command.

appnav-controller-group *ancgroupname*

no appnav-controller-group *ancgroupname*

Syntax Description

appnav-controller-group *ancgroupname*	Specifies the name of the ANCG to add to the service context. The ANCG must have been previously configured by the **service-insertion appnav-controller-group** command.

Command Default

No default behavior or values.

Command Modes

Service context configuration (config-scxt)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

A service context can have only one member ANCG.

Examples

The following is an example of this command:

```
service-insertion service-context appqoe/1
appnav-controller-group ACG-APPQOE
```

app-resource package-profile

To assign a DRE profile size to a device, use the **app-resource package-profile** command in app-hosting configuration mode. To remove the DRE profile assigned to a device, use the **no** form of this command.

app-resource package-profile *profile-size*

app-resource package-profile

Syntax Description

profile-size	The size of the DRE profile.

Command Default

The default DRE size specific to the device model is assigned.

Command Modes

App-hosting (config-app-hosting)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	This command was introduced.

Example

This example configures a small sized DRE profile on the device.

```
Device(config-app-hosting)# app-resource package-profile small
```

appqoe http-connect

To enable HTTP connect, use the **appqoe http-connect** command in the SD-WAN configuration mode. To disable HTTP connect, use the **no** form of this command.

appqoe http-connect enable [server-port] *port-number-1 [port-number-2] [port-number-3]*

no appqoe http-connect enable [server-port] *port-number-1 [port-number-2] [port-number-3]*

Table 8: Syntax Description

enable	Enables HTTP connect.
server-port	A number that identifies a specific process to which an internet or other network message is to be forwarded when it arrives at a server.
port-number	An HTTP connect request can be sent only using the following standard ports Port 80, 8080, and 8088

Command Default

HTTP connect is not enabled.

Command Modes

SD-WAN configuration (config-sdwan)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

This command enables HTTP connect. If you don't enter a standard port number, the default server-port number is assumed as 80.

Example

The following example shows how to enable HTTP connect.

```
Device(config)# sdwan
Device(config-sdwan)# appqoe
Device(config-appqoe)# http-connect enable server-port 80
```

appqoe tcpopt enable

To enable TCP optimization feature, use **appqoe tcpopt enable** command in Cisco SD-WAN configuration mode. To disable TCP optimization feature, use the **no** form of this command.

appqoe tcpopt enable

no appqoe tcpopt enable

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

SD-WAN configuration (config-sdwan)

Command History

Release	Modification
Cisco IOS XE Release 17.3.1a	TCP optimization support extended to CiscoISR4221, Cisco ISRv, and Cisco 1000 Series Integrated Services Routers.
Cisco IOS XE SD-WAN Release 16.12.1d	This feature optimizes TCP data traffic by decreasing any round-trip latency and improving throughput.

Usage Guidelines

TCP optimization fine tunes the processing of TCP data traffic to decrease round-trip latency and improve throughput. It is recommended that you configure TCP optimization on both the WAN Edge routers.

The command can be used to enable TCP optimization feature on WAN Edge routers.

Example

The following example shows how to enable TCP optimization feature on a WAN Edge:

```
Device(config)# sdwan
Device(config-sdwan)# appqoe tcpopt enable

Or

Device(config)# sdwan
Device(config-sdwan)# appqoe
Device(config-appqoe)# tcpopt enable
```

The following example show how to disable TCP optimization feature on a WAN Edge router.

```
Device(config)# sdwan
Device(config-sdwan)# no appqoe tcpopt enable

Or

Device(config)# sdwan
Device(config-sdwan)# appqoe
Device(config-appqoe)# no tcpopt enable
```

app-hosting

To start or activate application hosting, use the **app-hosting** command in privileged EXEC mode. To stop or deactivate application hosting, use the **no** form of this command.

app-hosting { **install** | **activate** | **start** | **stop** | **deactivate** | **uninstall** } **appid** *app-name*

Syntax Description

install	Installs an application from the specified location. An application can be installed from a local storage location.

activate	Validates all the application resource requests, and if all the resources are available, the application is activated; if not, the activation fails.
start	Starts and runs an application that has already been configured.
stop	Stops the DRE application.
deactivate	Deactivates all the resources allocated for the application.
uninstall	Uninstalls all the packaging and images stored. All the changes and updates to the application are also removed.
appid *app-name*	Specifies the name of the application.

Command Default

Application hosting is not enabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco vManage templates.

Usage Guidelines

The **start** command in application-hosting configuration mode is equivalent to the **app-hosting activate appid** and **app-hosting start appid** commands.

The **no start** command in application-hosting configuration mode is equivalent to the **app-hosting stop appid**and **app-hosting deactivate appid** commands.

Example

The following example shows how to install an application named Bangalore.

```
Device# app-hosting install appid Bangalore
```

The following example shows how to start app-hosting for an application named Bangalore

```
Device# app-hosting activate appid Bangalore
```

app-hosting appid

To configure an application and enter application-hosting configuration mode, use the **app-hosting app-id** command in global configuration mode.

To remove the application, use the **no** form of this command.

app-hosting app-id *app-name*

Syntax Description

app-name	Specifies a name for the application.

Command Default

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco vManage templates.

Usage Guidelines

Example

The following example shows how to configure an application with the name TEST, and enter application hosting configuration mode.

```
Device(config)# app-hosting appid TEST
Device(config-app-hosting)#
```

app-vnic

To configure a virtual interface gateway for application, use the **app-vnic** command in application hosting configuration mode. To remove the configuration, use the **no** form of this command.

app-vnic gateway0 [**virtualportgroup** *port-number* **guest-interface** *interface*]

Syntax Description

gateway0	Configures gateway0 as the VNIC gateway for the application.
virtualportgroup *port-number*	Configures a VirtualPortGroup interface for the gateway. Range: 0 to 31.
guest-interface *interface*	Configures a guest interface for the gateway. Range: 0 to 3.

Command Default The virtual network gateway is not configured

Command Modes Application hosting configuration (config-app-hosting)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco vManage templates.

Usage Guidelines After you configure the virtual network interface gateway of an application, the command mode changes to application-hosting gateway configuration mode. In this mode, you can configure the IP address of the guest interface.

Example

```
Device(config)# iox
Device(config)# app-hosting appid dreopt
Device(config-app-hosting)# app-vnic gateway0 virtualportgroup 3 guest-interface 1
Device(config-app-hosting-gateway)# guest-ipaddress 192.168.3.2 netmask 255.255.255.252
Device(config-app-hosting-gateway)# exit
Device(config-app-hosting)# start
Device(config-app-hosting)# exit
```

```
Device(config)# interface VirtualPortGroup3
Device(config-if)# no shutdown
Device(config-if)# ip address 192.168.3.1 255.255.255.252
Device(config-if)# exit
```

cluster-type

To specify the cluster type for a specific service-context, use the **cluster-type** command in service insertion context configuration mode. To remove this configuration, use the **no** form of this command.

cluster-type { **service-controller** | **integrated-service-node** }

no cluster-type

Syntax Description

service-controller	Specifies service controller as the cluster type.
integrated-service-node	Specifies integrated service node as the cluster type.

Command Default

Service cluster type is not configured.

Command Modes

Service insertion context (config-service-insertion-context)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Additional parameters qualified: **integrated-service-node**

Example

The following example shows how to enter the service insertion context configuration mode and specify service-controller as the cluster type.

```
Device(config)# service-insertion service-context appqoe CISCO
Device(config-service-insertion-context)# cluster-type service-controller
```

The following example shows how to enter the service insertion context configuration mode and specify integrated-service-node as the cluster type.

```
Device(config)# service-insertion service-context appqoe CISCO
Device(config-service-insertion-context)# cluster-type integrated-service-node
```

device-role

To specify the role of the device attached to the port, use the **device-role** command in service context configuration command mode.

device-role

Command Default The device role is host.

Command Modes Service context configuration (config-scxt)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

Examples The following is an example of this command:

```
service-insertion service-node-group appqoe SNG-APPQOE
device-role service-node
```

dreopt enable

To enable DRE optimization, use the **dreopt enable** command in AppQoE configuration mode.

dreopt enable

no dreopt [**enable**]

Syntax Description This command has no keywords or arguments.

Command Default DRE optimization is not enabled.

Command Modes AppQoE configuration (config-appqoe)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco vManage CLI templates

Example

The following example shows how to enable the AppQoE configure mode, and enable DRE optimization.

```
Device(config)# sdwan appqoe
Device(config-appqoe)# dreopt enable
```

dual-side optimization enable

To enable optimization of dual-side traffic, use the **dual-side optimization enable** command in SSL proxy configuration mode. To disable optimization of dual-side traffic, use the **no** form of this command.

dual-side optimization enable

no dual-side optimization

Syntax Description

This command has no keywords or arguments.

Command Default

Dual-side optimization is not enabled.

Command Modes

SSL proxy configuration (config-sslproxy)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco vManage CLI templates.

Example

```
sslproxy
 enable
 dual-side optimization enable
!
```

exporter

To export metrics from performance monitors to the collectors, use the **exporter** command in performance monitor configuration mode. To clear the configuration, use the **no** form of this command.

exporter destination { *destination-ip* [**source** *port*] | **local-sdwan source** *source* [**dscp** *value* | **vrf** *vrf-id*] }

no exporter destination

Syntax Description

destination *destination-ip*	Specifies the IP address of the collector.
source *source*	Specifies the source interface.
port *port*	(Optional) Specifies the port on the interface.
local-sdwan	Specifies that the performance monitor metrics be sent to Cisco vManage. Note that this option is only supported on features that support vManage as the collector. **Note** This keyword is not applicable to the Performance Monitor feature.
dscp *value*	(Optional) Specifies IP differentiated services code point (DSCP) values to match. Valid values are from 0 to 63.
vrf *vrf-id*	(Optional) Specifies that the export data packets should be sent to the VRF that is specified.

Command Default Performance monitor metrics are not exported to the collector.

Command Modes Performance monitor configuration (config-perf-mon)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Additional parameters qualified: **destination** *destination-ip*

Usage Guidelines After configuring performance monitor, use the **exporter** command to specify where the monitoring metrics should be exported.

The **local-sdwan** keyword is not applicable to the Performance Monitoring feature.

Example

The following example shows how to configure performance monitoring with the sdwan-performance profile, and then specify the destination IP, source interface, and port to export the monitoring metrics.

```
Device(config)# performance monitor context CISCO-MONITOR profile sdwan-performance
Device(config-perf-mon)# exporter destination 10.0.1.128 source GigabitEthernet9 port 2055
```

guest-ipaddress

To configure the IP address of the guest interface configured for application hosting (DRE), use the **guest-ipaddress** command in app hosting gateway configuration mode.

guest-ipaddress *ip-address* [**netmask** *mask*]

no guest-ipaddress *ip-address* [**netmask** *mask*]

Syntax Description

ip-address	The IP address that should be assigned to the guest interface.
netmask *mask*	Specifiest the netmask for the IP address.

Command Modes App hosting gateway configuration (config-app-hosting-gateway)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines After you configure the virtual network interface gateway of an application, the command mode changes to application-hosting gateway configuration mode. In this mode, you can configure the IP address of the guest interface.

Example

The following example assigns and IP address and netmask to the guest interface configured for app-hosting.

```
Device(config)# app-hosting appid dreopt
Device(config-app-hosting)# app-vnic gateway0 virtualportgroup 3 guest-interface 1
Device(config-app-hosting-gateway)# guest-ipaddress 192.168.3.2 netmask 255.255.255.252
```

iox

To enable DRE or UTD container, use the **iox** command in global configuration mode.

iox

no iox

Syntax Description

This command has no keywords or arguments.

Command Default

The container for DRE or UTD is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco vManage CLI templates.

Example

```
Device(config)# iox
Device(config)# app-hosting appid dreopt
Device(config-app-hosting)# app-vnic gateway0 virtualportgroup 3 guest-interface 1
Device(config-app-hosting-gateway)# guest-ipaddress 192.168.3.2 netmask 255.255.255.252
Device(config-app-hosting-gateway)# exit
Device(config-app-hosting)# start
Device(config-app-hosting)# exit
Device(config)# interface VirtualPortGroup3
Device(config-if)# no shutdown
Device(config-if)# ip address 192.168.3.1 255.255.255.252
Device(config-if)# exit
```

performance monitor apply

To apply performance monitor to a tunnel, use the **performance monitor apply** command in global configuration mode. To remove performance monitor from a tunnel, use the **no** form of this command.

performance monitor apply *context* { **color-all-dia** | **color-list** *color* | **sdwan-tunnel** }

no performance monitor apply *context*

Syntax Description

context	The name of the context for which the performance monitor should be applied.
color-all-dia	Applies performance monitor to all links in the Direct Internet Access (DIA) tunnel.
color-list *color*	Specifies the link color or colors to which the performance monitor should be applied.
sdwan-tunnel	Specifies that the performance monitor be applied to all SD-WAN tunnel interfaces.

Command Default

Performance monitor is not applied to any tunnel interfaces or links.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Additional parameters qualified: **sdwan-tunnel**

Usage Guidelines

The keywords **color-all-dia** and **color-list** are not applicable to the application performance monitor feature. These parameters are specific to ART monitoring for Cloud onRamp for SaaS applications.

Example

The following example shows how to apply performance monitor configuration on all SD-WAN tunnel interfaces globally.

```
Device(config)# performance monitor apply CISCO-MONITOR sdwan-tunnel
```

performance monitor context

To enable the performance monitor context on a specified interface, use the **performance monitor context** command in interface configuration mode. To remove performance monitor configuration, use the **no** form of this command.

performance monitor context *context-name* [**profile sdwan-performance**]

no performance monitor context *context-name* [**profile sdwan-performance**]

Syntax Description

context-name	Name of the performance monitor context name. The performance monitor context is used to enable performance monitor feature on the specified interface.
profile sdwan-performance	Specifies that the sdwan-performance profile should be applied to the class map specified for performance monitoring. **Note** This parameter is optional only if sdwan-performance profile is used to instantiate the performance monitor context.

Command Default Performance monitor is not configured.

Command Modes Interface configuration (config-if)

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines The keywords **profile** and **sdwan-performance** are optional only if the context name is generated when the sdwan-performance profile is applied.

Example

The following example shows how to enable performance monitor on Tunnel1.

```
interface Tunnel1
  performance monitor context CISCO-MONITOR
```

performance monitor sampling-rate

To monitor a specified number of flows as a sample, from the total flows being monitored, use the **performance monitor sampling-rate** command in global configuration mode. To remove the sampling rate, use the **no** form of this command

performance monitor sampling-rate *rate*

no performance monitor sampling-rate

Syntax Description

rate	Specifies the number of flows to be monitored from the total flows that performance monitor is applied to. Range: 2 to 32768

Command Default Sampling rate is not configured.

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

Example

The following example shows how to configure a sampling rate of 10 for the traffic being monitored:

```
Device(config)# performance monitor sampling-rate 10
```

platform resource

To configure a device to allocate cores to the service plane or the data plane, use the **platform resource** command in global configuration mode. To remove the core allocation configuration, use the no form of this command.

platform resource { **data-plane-heavy** | **service-plane-heavy** | **app-heavy** }

Syntax Description

data-plane-heavy	Allocates more cores to the data plane.
service-plane-heavy	Allocates more cores to the service plane.
app-heavy	Allocates more cores to the AppQoE service. **Note** Use this keyword to allocate more cores to the service plane of Cisco Catalyst 8000V instances on UCS E-Series servers.

Command Default

When this command is not configured, the supported Cisco Catalyst 8300 Series Edge Platforms are configured as service-plane heavy by default, and Cisco Catalyst 8000V Edge software is configured as data-plane heavy by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	A new keyword was added to this command: app-heavy

Usage Guidelines

If this command is not configured, the supported Cisco Catalyst 8300 Series Edge Platforms are configured as service-plane heavy by default, and Cisco Catalyst 8000V Edge software is configured as data-plane heavy by default. If you change the default configuration, you need to reboot the device for the updated configuration to take effect.

Example

The following example configures an external service node device as app-heavy.

```
Device(config)# platform resource app-heavy
```

rd

To specify a route distinguisher (RD) for a VPN routing and forwarding (VRF) instance, use the **rd**command in VRF configuration mode. To remove a route distinguisher, use the **no** form of this command.

rd *route-distinguisher*
no rd *route-distinguisher*

Syntax Description

route-distinguisher	An 8-byte value to be added to an IPv4 prefix to create a VPN IPv4 prefix.

Command Default

No RD is specified.

Command Modes

VRF configuration (config-vrf)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE rd command.

Examples

The following example shows how to configure a default RD:

```
vrf definition 100
rd 1:100
!
address-family ipv4
route-target export 1:100
route-target import 1:100
exit-address-family
!
```

sdwan appqoe dreopt enable

To enable DRE optimization, use the **sdwan appqoe dreopt enable** command in global configuration mode. To disable DRE, use the **no** form of this command.

sdwan appqoe dreopt enable

no sdwan appqoe dreopt enable

Command Default

DRE optimization is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco vManage templates.

Usage Guidelines

Example

The following example shows how to enable DRE optimization.

```
Device(config)# sdwan appqoe dreopt enable
```

service-insertion appqoe

To configure service nodes and a service controller to form a service node group, use the **service-insertion appqoe** command in interface configuration mode. To unconfigure the service node group, use the **no** form of this command.

service-insertion appqoe

no service-insertion appqoe

Syntax Description This command has no keywords or arguments.

Command Default No default behavior or values.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 17.5.1a	Command qualified for use in Cisco vManage CLI templates.

Examples

```
interface VirtualPortGroup2
no shutdown
ip address 192.168.2.1 255.255.255.0
service-insertion appqoe
```

service-insertion appnav-controller-group appqoe

To configure a service controller inside a service controller group, use the **service-insertion appnav-controller-group appqoe** command in global configuration mode.

To remove the service controller configuration, use the **no** form of this command.

service-insertion appnav-controller-group appqoe *group-name* [**appnav-controller** *ipv4-address* [**vrf** *vrf-id*] | **description** *description* [**appnav-controller** *ipv4-address* [**vrf** *vrf-id*]]]

no service-insertion appnav-controller-group appqoe

Syntax Description

group-name	Specifies the name of the AppQoE service-controller-group that the service controller is being configured under
appnav-controller *ipv4-address*	Specifies the IPv4 address of the AppQoE service controller
vrf *vrf-id*	Specifies the ID of the VRF to which this configuration is being applied.
description *description*	Provides a description for the AppQoE controller.

Command Default

No service controller is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command modified to enable applying the service-insertion configuration to a VRF.

Usage Guidelines

For the **service-insertion appnav-controller-group appqoe** configuration to take effect, you must create a VRF and configure interface VirtualPortGroup first.

Examples

The following example shows how to configure a service controller inside a controller group and connect service nodes to the controller:

```
config-transaction
 vrf definition 200
 !
 interface VirtualPortGroup2
  no shutdown
  ip address 192.168.2.1 255.255.255.0
  service-insertion appqoe
  !
 service-insertion appnav-controller-group appqoe ACG-APPQOE
  appnav-controller 198.51.100.1 vrf 200
  !
 service-insertion service-node-group appqoe SNG-APPQOE
  service-node 192.0.2.2
  service-node 192.0.2.3
  service-node 192.0.2.4
  service-node 192.0.2.5
  !
 service-insertion service-context appqoe/1
  appnav-controller-group ACG-APPQOE
  service-node-group SNG-APPQOE
  cluster-type service-controller
  enable
  vrf default
  !
```

service-insertion service-node-group appqoe

To configure a supported device as an external AppQoE service node, use the **service-insertion service-node-group appqoe** command in global configuration mode.

To remove the service node configuration, see the **no** form of this command.

service-insertion service-node-group appqoe *group-name* [**description** *description*] [**device-role service-node**] [**node-discovery enable**] [**service-node** *ipv4-address*]

no service-insertion service-node-group appqoe

Syntax Description

group-name	Specifies the name of the appqoe service-node-group that the service node is being configured under
device-role service-node	(Optional) Configures the supported device with the service-node role
node-discovery enable	(Optional) Enables discovery for the service node
service-node *ipv4-address*	(Optional) Specifies the IPv4 address of the service node

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command modified. Support was added for the keywords **device-role service-node**, which enables you to configure a device as an external service node.

Usage Guidelines

The parameters after **service-insertion service-node-group appqoe** *group-name* are optional and can be entered in any order.

Examples

The following example shows how to configure a service node in a service node group.

```
config-transaction
 service-insertion service-node-group appqoe SNG-APPQOE
  device-role service-node
  service-node 192.168.2.2
  !
```

start (app-hosting)

To start the DRE service, use the **start** command in app-hosting configuration mode. To stop the DRE service, use the **no** form of this command.

start

no start

Syntax Description This command has no keywords or arguments.

Command Default The DRE service does not start.

Command Modes App hosting gateway configuration (config-app-hosting)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco vManage CLI templates.

Example

```
app-hosting appid dreopt
app-resource package-profile extra-large
app-vnic gateway0 virtualportgroup 3 guest-interface 1
guest-ipaddress 192.168.3.2 netmask 255.255.255.252
!
start
```

traffic-monitor

To specify the type of traffic that sdwan-performance monitoring profile monitors, use the **traffic-monitor** command in performance monitor configuration mode. To clear the types of traffic being monitored, use the **no** form of this command.

traffic-monitor { **application-response-time** | **media** | **art-cor-saas** } [**class-and** *class-map* [**ipv4**]] [**class-replace** *class-map*]

no traffic-monitor [**application-response-time** | **media** | **art-cor-saas**] [**class-and** | **class-replace**]

Syntax Description

application-response-time	Specifies that application response time (ART) be monitored for the specified traffic.
media	Specifies that media traffic be monitored.
art-cor-saas	Specifies that ART be monitored for traffic specific to Cloud onRamp for SaaS.
class-and *class-map*	Specifies that traffic monitoring be filtered by additional class maps specified.
class-replace *class-map*	Specifies that the customized class-map replace the default class-map, which is automatically created when you enable the sdwan-performance profile for monitoring.
ipv4	Specifies that only IPv4 flows be monitored. **Note** For the Application Performance Monitor feature introduced in Cisco IOS XE Catalyst SD-WAN Release 17.5.1a, IPv4 is enabled by default.

Command Default Performance monitoring is not applied to specific traffic type.

Command Modes Performance monitor configuration (config-perf-mon)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Additional parameters qualified: **application-response-time** and **media**

Usage Guidelines After configuring performance monitor, use the **traffic-monitor** command to specify which traffic type should be monitored.

Example

The following example show how to configure traffic monitoring by ART for media monitoring.

```
Device(config)# performance monitor context CISCO-MONITOR profile sdwan-performance
Device(config-perf-mon)# traffic-monitor application-response-time
Device(config-perf-mon)# traffic-monitor media
```

vrf (service-insertion-context)

To specify the VRF to which the AppQoE service should be applied, use the **vrf** command in service-insertion-context configuration mode. To remove the AppQoE service from the VRF, use the **no** form of this command.

vrf global

no vrf global

Syntax Description

global	Applies the AppQoE service to the global VRF.

Command Default AppQoE service is not applied to the VRF.

Command Modes Service insertion context (config-service-insertion-context)

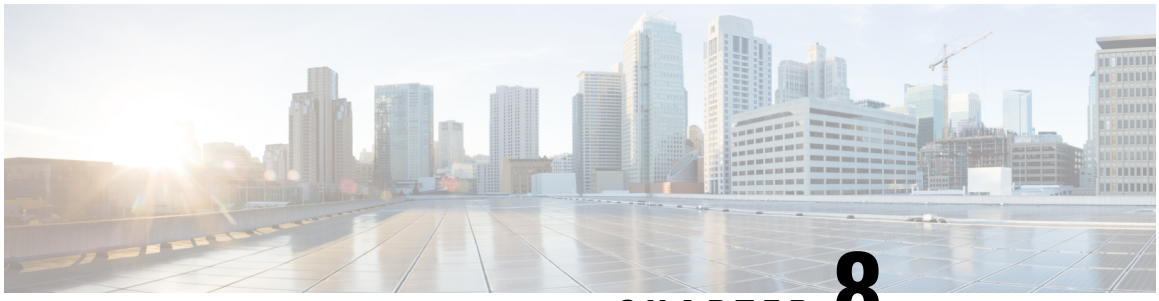
Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

Example

```
service-insertion service-context appqoe/1
 appnav-controller-group ACG-APPQOE
 service-node-group SNG-APPQOE
```

```
 cluster-type integrated-service-node
 enable
 vrf global
!
```



CHAPTER 8

ATM-native Commands

- encapsulation (ATM), on page 71
- interface ATM, on page 73
- oam-pvc, on page 74
- oam retry, on page 75
- pvc, on page 76
- service-policy, on page 77
- vbr-nrt, on page 78
- Physical and Logical ATM Interface Commands, on page 79
- bridge-dot1q encap, on page 79
- dialer pool-member, on page 79
- ip mtu, on page 80
- load-interval, on page 81
- protocol (ATM), on page 82

encapsulation (ATM)

To configure the ATM adaptation layer (AAL) and encapsulation type for an ATM virtual circuit (VC), VC class , VC, bundle, or permanent virtual circuit (PVC) range, use the **encapsulation**command in the appropriate mode. To remove an encapsulation type, use the **no** form of this command.

encapsulation { **aal5mux** *protocol* | **aal5snap** }

no encapsulation

Syntax Description

aal5mux	Specifies the AAL and encapsulation type for multiplex (MUX)-type VCs. A protocol must be specified when you use this encapsulation type.

protocol	Protocol type being used by the multiplex (MUX)-encapsulated VC. Values for the *protocol*argument are as follows: • **appletalk** --AppleTalk protocol. • **bridge ieee8023** --Ethernet LAN protocol. • **decnet** --DECnet protocol. • **frame-relay** --Frame Relay-ATM Network Interworking (FRF.5) on the Cisco MC3810. • **fr-atm-srv** --Frame Relay-ATM Service Interworking (FRF.8) on the Cisco MC3810. • **ip** --IP protocol. • **ipx** --Internet Packet Exchange (IPX) protocol. • **ppp Virtual-Template** *template-number* - Internet Engineering Task Force (IETF)-compliant PPP over ATM. Use the **virtual-template** *template-number* option to identify the virtual template. This keyword is supported on ATM PVCs only. • **pppoe** --PPP over Ethernet. • **voice** --Voice over ATM.
aal5snap	Specifies the AAL and encapsulation type that supports Inverse Address Resolution Protocol (ARP). Logical link control/Subnetwork Access Protocol (LLC/SNAP) precedes the protocol datagram.

Command Default

The global default encapsulation option is **aal5snap**.

Command Modes

ATM PVC configuration (config-if-pvc)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates. The **aal5snap** command option is qualified.
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Command qualified for use in Cisco vManage CLI templates. The **aal5mux** *protocol* command option is qualified.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `encapsulation (ATM)` command.

MUX-Type Encapsulation on a VC Example

```
Device(config)# interface ATM 0/3/0
Device(config-subif)# no shutdown
Device(config-subif)# pvc 0/1
Device(config-if-pvc)# encapsulation aal5mux ppp Virtual-Template 1
```

SNAP Encapsulation Example

```
Device(config)# interface ATM 0/3/0.1 point-to-point

Device(config-subif)# ip address 10.0.0.0 255.255.255.252
Device(config-subif)# ip mtu 1496
Device(config-subif)# no shutdown
Device(config-subif)# pvc 0/100
Device(config-if-pvc)# bridge-dot1q encap 1
Device(config-if-pvc)# encapsulation aal5snap
```

MUX Encapsulation Example

```
Device(config)# interface ATM 0/2/0.1 point-to-point
Device(config-subif)# pvc 0/1
Device(config-if-pvc)# encapsulation aal5mux ppp dialer
```

interface ATM

To configure an ATM interface and enter interface configuration mode, use the **interface ATM** command in global configuration mode. To remove an ATM interface configuration, use the no form of this command.

interface atm *interface-number* [**.** *subinterface-number* { **multipoint** | **point-to-point** }]
no interface ATM *interface-number*

Syntax Description

interface-number	Specifies a (physical) ATM interface (for example, 3/0).
. *subinterface-number*	(Optional) Specifies a subinterface number. A dot (.) must be used to separate the *interface-number* from the *subinterface-number* (for example 2/0.1).
multipoint	(Optional) Specifies multipoint as the interface type for which a subinterface is to be created.
point-to-point	(Optional) Specifies point-to-point as the interface type for which a subinterface is to be created.

Command Default

No ATM interfaces are configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `interface atm` command.

Examples

For physical ATM interface 3/0, the following command creates an ATM subinterface having subinterface number 1:

```
Device(config)# interface ATM 3/0.1
```

Examples

For physical ATM interface 0/2/0.1, the following command creates an ATM subinterface:

```
Device(config)# interface ATM 0/2/0.1
```

Examples

The following command specifies point-to-point as the interface type for which an ATM subinterface is created:

```
Device(config)# interface ATM 0/2/0.1 point-to-point
```

oam-pvc

To enable end-to-end F5 Operation, Administration, and Maintenance (OAM) loopback cell generation and OAM management for an ATM permanent virtual circuit (PVC), virtual circuit (VC) class, or label-controlled ATM (LC-ATM) VC, use the **oam-pvc** command in the appropriate command mode. To disable generation of OAM loopback cells and OAM management, use the **no** form of this command.

ATM VC
oam-pvc [*frequency* | **manage** [*frequency*]]
no oam-pvc [*frequency* | **manage** [*frequency*]]

Syntax Description

frequency	(Optional) Specifies the time delay between transmittals of OAM loopback cells, in seconds. For ATM VCs , the range is 0 to 600, and the default is 10.
manage	(Optional) for ATM VCs; Enables OAM management. The default is disabled.

Command Default

OAM management is disabled.

Command Modes

ATM VC class configuration (config-vc-class)
ATM VC configuration (config-if-atm-vc)
ATM PVC configuration (config-if-pvc)
Control-VC configuration (cfg-mpls-atm-cvc)
PVC-in-range configuration (cfg-if-atm-range-pvc)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE oam-pvc command.

Examples

The following example shows OAM management on an LC-ATM interface with a transmission frequency of 2 seconds:

```
Router(config)# interface ATM 0/2/0.1 point-to-point
Router(config-subif)# pvc 0/1
Router(config-if-pvc)# oam-pvc manage 2
```

oam retry

To configure parameters related to Operation, Administration, and Maintenance (OAM) management for an ATM permanent virtual circuit (PVC), switched virtual circuit (SVC), VC class, or VC bundle, or label-controlled ATM (LC-ATM) VC, use the **oam retry** command in the appropriate command mode. To remove OAM management parameters, use the **no** form of this command.

oam retry *up-count down-count retry-frequency*
no oam retry

Syntax Description

up-count	Number of consecutive end-to-end F5 OAM loopback cell responses that must be received in order to change a connection state to up. This argument does not apply to SVCs.
down-count	Number of consecutive end-to-end F5 OAM loopback cell responses that are not received in order to change the state to down or tear down an SVC connection.
retry-frequency	The frequency (in seconds) at which end-to-end F5 OAM loopback cells are transmitted when a change in the up/down state is being verified. For example, if a PVC is up and a loopback cell response is not received after the *retry-frequency* (in seconds) argument is specified using the **oam-pvc** command, loopback cells are sent at the *retry-frequency* to verify whether the PVC is down.

Command Default

ATM PVCs and SVCs

up-count : 3*down-count*: 5*retry-frequency*: 1 second

LC-ATM VCs

up-count : 2*down-count*: 2*retry-frequency*: 2 seconds

Command Modes

Bundle configuration mode (for a VC bundle)
Control-VC configuration (for an LC-ATM VC)
Interface-ATM-VC configuration (for an ATM PVC or SVC)
PVC range configuration (for an ATM PVC range)
PVC-in-range configuration (for an individual PVC within a PVC range)
VC-class configuration (for a VC class)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE oam retry command.

Examples

The following example shows how to configure the OAM management parameters with an up count of 3, a down-count of 3, and the retry frequency set at 10 seconds:

```
Device(config)# interface ATM 0/2/0.1 point-to-point
Device(config-subif)# pvc 0/1
Device(config-if-pvc)# oam retry 3 3 10
```

pvc

To create or assign a name to an ATM permanent virtual circuit (PVC), to specify the encapsulation type on an ATM PVC, and to enter ATM virtual circuit configuration mode, use the **pvc** command in interface configuration mode or subinterface configuration mode. To remove an ATM PVC from an interface, use the **no** form of this command.

pvc *vpi/vci*

Syntax Description

vpi	Specifies the ATM network virtual path identifier (VPI) for this PVC. The slash is required. This value defaults to 0 if no value is given for *vpi/*. The arguments *vpi* and *vci* cannot both be set to 0; if one is 0, the other cannot be 0.
vci	Specifies the ATM network virtual channel identifier (VCI) for this PVC. The range of valid values is 0 to 1 less than the maximum value set for this interface by the atm vc-per-vp command. Lower values from 0 to 31 are usually reserved for specific traffic such as: F4 Operation Administration and Maintenance (OAM), SSL VPN Client (SVC) signaling, Interim Local Management Interface (ILMI), and so on.; and should not be used. The VCI value is a 16-bit field in the header of the ATM cell. The VCI value is unique only on a single link, not throughout the ATM network, because it has local significance only. A value that is out of range causes an “unrecognized command” error message. The arguments vpi and vci cannot both be set to 0; if one is 0, the other cannot be 0.

Command Default

No PVC is defined.

Command Modes

Interface configuration (config-if)
Subinterface configuration (config-subif)

Usage Guidelines

This command is used to create or assign a name to an ATM permanent virtual circuit (PVC), to specify the encapsulation type on an ATM PVC, and to enter ATM virtual circuit configuration mode.

When a PVC is defined, the global default of the encapsulation command applies (aal5snap). Use the **pvc** command to configure a single ATM VC only, not a VC that is a bundle member.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Examples

The following example specifies the output PCR for an ATM PVC to be 100,000 kbps, the output SCR to be 50,000 kbps, and the output MBS to be 64:

```
Device# config-t
Device(config)# interface ATM 0/2/0
Device(config-if)# no shut
Device(config-if)# interface ATM 0/2/0.1 point-to-point
Device(config-subif)# pvc 0/32
```

service-policy

To attach a policy map to an input interface or an output interface, use the **service-policy** command in the appropriate configuration mode. To remove a service policy from an input or output interface, use the **no** form of this command.

service-policy output *policy-map-name*
no service-policy

Syntax Description

output	Attaches the specified policy map to the output interface or output VC.
policy-map-name	The name of a service policy map (created using the **policy-map** command) to be attached. The name can be a maximum of 40 alphanumeric characters in length.

Command Default

No service policy is specified. A control policy is not applied to a context. No policy map is attached.

Command Modes

Interface configuration (config-if)

Subinterface configuration (config-subif)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For the usage guidelines, see service-policy.

Examples

```
Device(config)# interface GigabitEthernet 1
Device(config-if)# service-policy output  policy_1
```

Examples

```
Device(config)# interface ATM 0/2/0.1 point-to-point
Device(config-subif)# service-policy output  policy_1
```

vbr-nrt

To configure the variable bit rate-nonreal time (VBR-NRT) quality of service (QoS) and specify output peak cell rate (PCR), output sustainable cell rate (SCR), and output maximum burst cell size for an ATM permanent virtual circuit (PVC), PVC range, switched virtual circuit (SVC), VC class, or VC bundle member, use the **vbr-nrt** command in the appropriate command mode. To remove the VBR-NRT parameters, use the **no** form of this command.

vbr-nrt *output-pcr output-scr* [*output-maxburstsize*] [*input-pcr*] [*input-scr*] [*input-maxburstsize*]
no vbr-nrt *output-pcr output-scr output-maxburstsize* [*input-pcr*] [*input-scr*] [*input-maxburstsize*]

Syntax Description

output-pcr	The output PCR, in kilobytes per second (kbps).
output-scr	The output SCR, in kbps.
output-maxburstsize	The output maximum burst cell size, expressed in number of cells.
input-pcr	(Optional for SVCs only) The input PCR, in kbps.
input-scr	(Optional for SVCs only) The input SCR, in kbps.
input-maxburstsize	(Optional for SVCs only) The input maximum burst cell size, expressed in number of cells.

Command Default

Unspecified bit rate (UBR) QoS at the maximum line rate of the physical interface is the default.

Command Modes

ATM PVC-in-range configuration (for an individual PVC within a PVC range)
ATM PVC range configuration (for an ATM PVC range)
ATM PVP configuration
Bundle-vc configuration (for ATM VC bundle members)
Interface-ATM-VC configuration (for an ATM PVC or SVC)
VC-class configuration (for a VC class)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE vbr-nrt command.

Examples

The following example specifies the output PCR for an ATM PVC to be 48 kbps, the output SCR to be 1 kbp:

```
Device(config)# interface ATM 0/2/0.1 point-to-point
Device(config-subif)# pvc 0/1
Device(config-if-pvc)# vbr-nrt 48 1
```

Physical and Logical ATM Interface Commands

bridge-dot1q encap

To add a VLAN ID to an ATM permanent virtual circuit (PVC) over an ATM xDSL link or a PVC configured using Route-Bridge Encapsulation (RBE), use the **bridge-dot1q encap** command in ATM PVC configuration mode. To prevent a VLAN ID from being sent across the link, use the **no** form of this command.

bridge-dot1q encap *outgoing-vlan-id*
no bridge-dot1q encap *outgoing-vlan-id*

Syntax Description

outgoing-vlan-id	The VLAN ID to be carried over an ATM xDSL link. The valid value of the VLAN ID can range from 1 to 4094.

Command Default

If this command is not used a VLAN ID is not added to an ATM PVC configured over an ATM xDSL link or a PVC configured using RBE.

Command Modes

ATM PVC configuration (config-if-pvc)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

You can configure only one 802.1Q VLAN tag under a PVC.

If the incoming packet at the Fast Ethernet port contains an ingress 802.1Q tag, the ingress 802.1Q tag is replaced by the egress 802.1Q tag while the packet is forwarded over an ATM xDSL link.

The **bridge-dot1q encap** *outgoing-vlan-id* command can also be used to tag packets on a PVC that is configured on an RBE subinterface.

The Transporting 802.1Q Tag over PVC feature is supported only for ATM Adaptation Layer 5 Subnetwork Protocol Access Protocol (AAL5-SNAP) encapsulation.

Examples

```
Device(config)# interface ATM 0/3/0.1 point-to-point

Device(config-subif)# ip address 10.0.0.0 255.255.255.252
Device(config-subif)# ip mtu 1496
Device(config-subif)# no shutdown
Device(config-subif)# pvc 0/100
Device(config-if-pvc)# bridge-dot1q encap 1
```

dialer pool-member

To configure a physical interface to be a member of a dialer profile dialing pool, use the **dialer pool-member** command in interface configuration mode. To remove the configuration, use the **no** form of this command.

dialer pool-member *number*

no dialer pool-member

Syntax Description

number	Dialing pool number. Range is from 1 to 255.

Command Default

The interface is not a member of a dialer profile dialing pool.

Command Modes

ATM PVC configuration (config-if-pvc)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

The common dialing pool number used in the **dialer pool** command and in the **dialer pool-member** command links the physical interface and dialer interface configurations.

For more usage guidelines, see the Cisco IOS XE dialer pool-member command.

Example

```
Device(config)# interface ATM 0/3/0/0.1 point-to-point
Device(config-subif)# pvc 0/100
Device(config-if-pvc)# dialer pool-member 1
```

ip mtu

To set the maximum transmission unit (MTU) size of IP packets that are sent on an interface, use the **ip mtu** command in interface configuration mode. To restore the default MTU size, use the **no** form of this command.

ip mtu *bytes*
no ip mtu

Syntax Description

bytes	MTU size, in bytes.

Command Default

The default MTU value depends on the interface type.

Table 9: Default MTU Values by Interface Type

Interface Type	Default MTU (Bytes)
ATM	4470
Ethernet	1500
FDDI	4470
High-Speed Serial Interface High Speed Access (HSSI HSA)	4470

Interface Type	Default MTU (Bytes)
Serial	1500
Token Ring	4464
VRF-Aware Service Infrastructure (VASI)	9216

Command Modes

Interface configuration (config-if)
Subinterface configuration (config-subif)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For the usage guidelines, see the IOS XE ip mtu command.

Examples

```
Device(config)# interface GigabitEthernet 1
Device(config-if)# ip mtu 1500
```

```
Device(config)# interface ATM 0/2/0.1 point-to-point
Device(config-if)# ip mtu 1500
```

load-interval

To change the length of time for which data is used to compute load statistics, use the **load-interval** command in the interface or sub-interface configuration mode. To revert to the default setting, use the **no**form of this command.

load-interval *seconds*
no load-interval *seconds*

Syntax Description

seconds	Length of time for which data is used to compute load statistics. Value is a multiple of 30, from 30 to 600 (30, 60, 90, 120, and so on). The default is 300 seconds.

Command Default

Enabled

Command Modes

Interface configuration (config-if)

Sub-interface configuration (config-subif)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For the usage guidelines, see load-interval.

Interface Example

```
Device(config)# interface ATM 0/3/0.1 point-to-point
Device(config-subif)# load-interval 30
```

protocol (ATM)

To configure a static map for an ATM permanent virtual circuit (PVC), switched virtual circuit (SVC), or virtual circuit (VC) class or to enable Inverse Address Resolution Protocol (ARP) or Inverse ARP broadcasts on an ATM PVC, use the **protocol** command in the appropriate mode. To remove a static map or disable Inverse ARP, use the **no** form of this command.

protocol *protocol* **dialer**
no protocol *protocol*

Syntax Description

protocol	Choose one of the following values: • **aarp** —AppleTalk ARP • **appletalk**—AppleTalk • **arp**—IP ARP • **bridge**—bridging • **bstun**—block serial tunnel • **cdp**—Cisco Discovery Protocol • **clns**—ISO Connectionless Network Service (CLNS) • **clns_es**—ISO CLNS end system • **clns_is**—ISO CLNS intermediate system • **cmns**—ISO CMNS • **compressedtcp**—Compressed TCP • **decnet**—DECnet • **decnet_node**—DECnet node • **decnet_prime_router**—DECnet prime router • **decnet_router-l1**—DECnet router L1 • **decnet_router-l2**—DECnet router L2 • **dlsw**—data link switching • **ip**—IP**ipx**—Novell IPX • **llc2**—llc2 • **pad**—packet assembler/disassembler (PAD) links • **ppp**—Point-to-Point Protocol carried on the VC • **pppoe**—PPP over Ethernet • **qllc**—Qualified Logical Link Control protocol • **rsrb**—remote source-route bridging • **snapshot**—snapshot routing support • **stun**—serial tunnel
dialer	Specifies a dialer interface that an accept-dialout virtual private dialup network (VPDN) subgroup will use to dial out calls.

Command Default

Inverse ARP is enabled for IP and IPX if the protocol is running on the interface and no static map is configured.

Command Modes

Interface-ATM-VC configuration (for an ATM PVC or SVC)

VC-class configuration (for a VC class)

PVC range configuration (for an ATM PVC range)

PVC-in-range configuration (for an individual PVC within a PVC range)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `protocol (ATM)` command.

Examples

The following example creates a static map on a VC, indicates that 192.0.2.2 is connected to this VC, and sends ATM pseudobroadcasts:

```
protocol ip 192.0.2.2 broadcast
```

The following example enables Inverse ARP for IPX and does not send ATM pseudobroadcasts:

```
protocol ipx inarp no broadcast
```

The following example removes a static map from a VC and restores the default behavior for Inverse ARP (see the “Command Default” section described above):

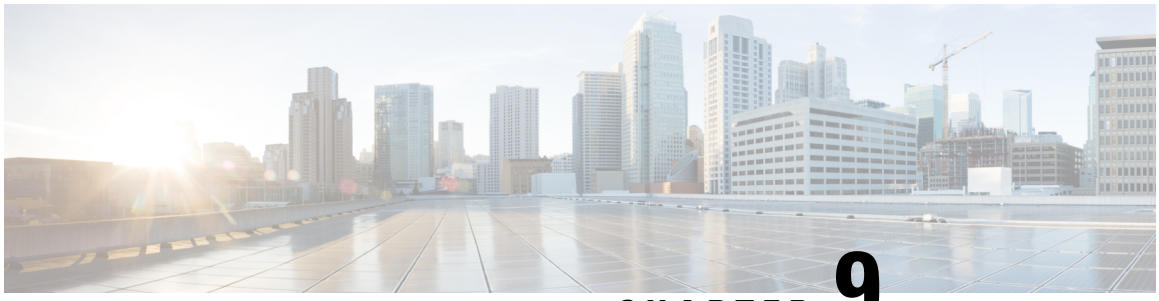
```
no protocol ip 192.0.2.2
```

In the following example, the VC carries PPP traffic and its associated parameters.

```
protocol ppp 192.0.2.2 virtual-template
```

In the following example, the VC carries PPP traffic to a dialer interface .

```
interface ATM 0/2/0.1 point-to-point
pvc 0/1
protocol ppp dialer
```



CHAPTER 9

BFD Commands

- alarms alarm bfd-state-change syslog, on page 85
- bfd app-route, on page 86
- bfd enhanced-app-route, on page 87
- bfd color, on page 88
- hello-interval, on page 89
- pmtu-discovery, on page 89

alarms alarm bfd-state-change syslog

To enable the BFD syslog messages, use the **alarms alarm bfd-state-change syslog** command in system configuration mode. To disable BFD syslog messages, use the **no** form of this command.

alarms alarm bfd-state-change syslog
no alarms alarm bfd-state-change syslog

Syntax Description

bfd-state-change	BFD state change.
syslog	Enables syslog for this feature.

Command Default

If the command is not used, the BFD state change syslog messages are not reported in the console.

Command Modes

System configuration (config-system)

Command History

Release	Modification
Cisco IOS XE Release 17.6.3	This command was introduced.

Usage Guidelines

When the command is configured, if there is a BFD state change event in the device , then the BFD state change syslog message is displayed for every session.

The following example shows how to enable BFD syslog messages:

```
Device(config)# system
Device(config-system)# alarms alarm bfd-state-change syslog
Device(config-alarm-bfd-state-change)# commit
```

The following example shows how to disable BFD syslog messages:

```
Device(config-system)# no alarms alarm bfd-state-change syslog
Device(config-system)# commit
Commit complete.
```

bfd app-route

To configure Bidirectional Forwarding Protocol timers used by application-aware routing, use the **bfd app-route** command. To disable, use the **no** form of this command.

bfd app-route { **multiplier** | **poll-interval** }
no bfd app-route

Syntax Description

multiplier *number*	Multiplier for the Polling Interval: Value to multiply the poll interval by to set how often application-aware routing acts on the data plane tunnel statistics to figure out the loss and latency and to calculate new tunnels if the loss and latency times do not meet configured SLAs. Range: 1 through 6 Default: 6
poll-interval *milliseconds*	Polling Interval: How often BFD polls all data plane tunnels on a vEdge router to collect packet latency, loss, and other statistics to be used by application-aware routing. Range: 1 through 4,294,967,295 ($2^{32} – 1$) milliseconds Default: 600,000 milliseconds (10 minutes)

Command Default

None.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

Note BFD multiplier does not account for processing delays during BFD convergence. There is a delay of a few additional seconds for BFD convergence to complete.

Example

Change the polling interval and multiplier to use for application-aware routing:

```
bfd app-route multiplier 6
 bfd app-route poll-interval 4294967295
```

bfd enhanced-app-route

To enable enhanced PfR measurements for SLA enforcement, use the **bfd enhanced-app-route enable** command. To disable enhanced PfR measurements for SLA enforcement, use the **no** form of this command.

bfd enhanced-app-route enable
no bfd enhanced-app-route enable

pfr-poll-interval	This command is used for SLA enforcement and switchover. Default poll-interval: 10 milliseconds
pfr-multiplier *number*	This command is used for SLA enforcement and switchover. Default multiplier (aggressive mode): 6
ignore-local-loss	This command is used to ignore local loss on the router which is caused by QOS queues. By default, loss includes both local and WAN loss.

Command Default

None

Command Modes

Global configuration (config)

Release	Modification
Cisco IOS XE Release 17.12.1a	This command was introduced.
Cisco IOS XE Release 17.12.6, 17.15.5 and 17.18.2 onwards	The **ignore-local-loss** command is available.

Usage Guidelines

Enabling the application-aware routing feature on a Cisco IOS XE Catalyst SD-WAN device requires you to enable the PfR CLI on both the remote Cisco IOS XE Catalyst SD-WAN device and the local Cisco IOS XE Catalyst SD-WAN device.

bfd color

To configure the Bidirectional Forwarding Protocol timers used on transport tunnels use the **bfd color** command. To disable this command, use the **no** form of this command.

bfd color { **mpls** | **lte** | **3g** }
no bfd color

Syntax Description

color *color*	Identifier for the Transport Tunnel: Transport tunnel for data traffic moving between vEdge routers. The color identifies a specific WAN transport provider. Values: **3g**, **biz-internet**, **blue**, **bronze**, **custom1**, **custom2**, **custom3**, **default**, **gold**, **green**, **lte**, **metro-ethernet**, **mpls**, **private1** through **private6**, **public-internet**, **red**, **silver** Default: **default**

Command Default

None.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

The following are examples for this command

```
bfd color mpls
  hello-interval 300000
  no pmtu-discovery
  multiplier     60
 !


 bfd color lte
  hello-interval 300000
  pmtu-discovery
  multiplier     60
 !


 bfd color 3g
  hello-interval 300000
  no pmtu-discovery
  multiplier     60
```

hello-interval

To set the BFD Hello interval for a transport color, use the **hello-interval** command in BFD transport color configuration mode. To remove the BFD Hello interval, use the **no** form of this command.

hello-interval *milliseconds*

Syntax Description

milliseconds	Specifies how often BFD sends Hello packets. Range: 100 through 310000 milliseconds

Command Default

BFD Hello interval is set to 1000 milliseconds (1 second) by default.

Command Modes

Transport color configuration (config-color-*transport-color*)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

BFD uses Hello packets to detect the liveness and faults on a connection. BFD Hello Interval packet is sent at the default interval of 1000 milliseconds on all connections. This command can be used to change the hello interval for a transport color.

Example

The following example shows how to configure the hello-interval on the transport MPLS to 3 seconds (3000 milliseconds).

```
Device(config)# bfd color mpls
Device(config-color-mpls)# hello-interval 3000
```

pmtu-discovery

To enable Path MTU (PMTU) discovery for a transport color, use the **pmtu-discovery** command in BFD transport color configuration mode. To disable PMTU discovery, use the **no** form of this command.

pmtu-discovery

no pmtu-discovery

Command Default

PMTU discovery is disabled.

Command Modes

Transport color configuration (config-color-*transport-color*)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

When PMTU discovery is enabled, the path MTU for the connection is checked periodically, about once in twenty minutes, and it is updated dynamically. When PMTU discovery is disabled, the expected connection MTU is 1472 bytes, but the effective connection MTU is 1468 bytes. Use this command to enable PMTU discovery.

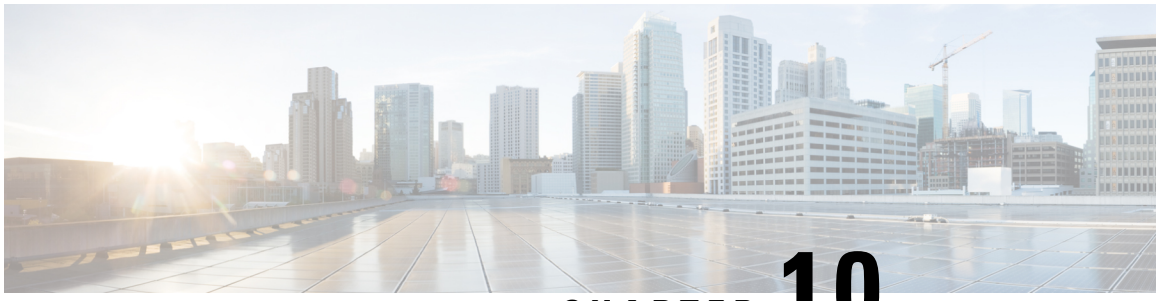
Example

The following example shows how to enable PMTU discovery on the transport MPLS.

```
Device(config)# bfd color mpls
Device(config-color-mpls)# pmtu-discovery
```

Related Commands

Command	Description
hello-interval	Set the interval at which Hello Packets are sent. Range: 100 to 310000 milliseconds.
multiplier	Sets the maximum number of attempts. Range: 1 to 60.



CHAPTER 10

BGP Commands

- address-family ipv4 (BGP), on page 92
- address-family ipv6, on page 93
- aggregate-address, on page 93
- bandwidth (policy-map class), on page 94
- bgp always-compare-med, on page 95
- bgp bestpath as-path multipath-relax, on page 96
- bgp bestpath compare-routerid, on page 97
- bgp bestpath med missing-as-worst, on page 98
- bgp deterministic-med, on page 98
- bgp graceful-restart, on page 99
- bgp log-neighbor-changes, on page 99
- bandwidth remaining ratio, on page 100
- class (policy-map), on page 101
- distance bgp, on page 102
- exit-address-family (bgp), on page 103
- maximum-paths eibgp, on page 104
- neighbor advertise-map, on page 104
- neighbor advertisement-interval, on page 105
- neighbor description, on page 106
- neighbor ebgp-multihop, on page 107
- neighbor ha-mode graceful-restart, on page 108
- neighbor maximum-prefix (BGP), on page 108
- neighbor next-hop-self, on page 109
- neighbor password, on page 110
- neighbor remote-as, on page 111
- neighbor route-map, on page 112
- neighbor send-community, on page 113
- neighbor shutdown, on page 113
- neighbor timers, on page 114
- network (BGP and multiprotocol BGP), on page 115
- police (percent), on page 115
- policy-map, on page 116
- priority level, on page 117

- redistribute (IP), on page 118
- redistribute omp (bgp) , on page 120
- router bgp, on page 121
- timers bgp, on page 122

address-family ipv4 (BGP)

To enter address family or router scope address family configuration mode to configure a routing session using standard IP Version 4 (IPv4) address prefixes, use the **address-family ipv4** command in router configuration or router scope configuration mode. To exit address family configuration mode and remove the IPv4 address family configuration from the running configuration, use the **no** form of this command.

address-family ipv4 [**unicast**] [**vrf** *vrf-name*]
no address-family ipv4 [**unicast**] [**vrf** *vrf-name*]

Syntax Description

unicast	(Optional) Specifies IPv4 unicast address prefixes. This is the default.
vrf *vrf-name*	(Optional) Specifies the name of the VPN routing and forwarding (VRF) instance to associate with subsequent IPv4 address family configuration mode commands.

Command Default

IPv4 address prefixes are not enabled.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `address-family ipv4` (BGP) command.

Examples

The following example places the device in address family configuration mode for the IPv4 address family:

```
router bgp 50000
 address-family ipv4
```

The following example places the device in address family configuration mode, specifies unicast address prefixes for the IPv4 address family, and specifies 1 as the VRF instance to associate with subsequent address family configuration mode commands:

```
router bgp 64496
 address-family ipv4 unicast vrf 1
```

address-family ipv6

To enter address family configuration mode for configuring routing sessions, such as BGP, that use standard IPv6 address prefixes, use the **address-family ipv6** command in router configuration mode. To disable address family configuration mode, use the **no** form of this command.

address-family ipv6 [**vrf** *vrf-name*] [**unicast**]
no address-family ipv6 [**unicast**] [**vrf** *vrf-name*]

Syntax Description

unicast	(Optional) Specifies IPv4 unicast address prefixes. This is the default.
vrf *vrf-name*	(Optional) Specifies the name of the VPN routing and forwarding (VRF) instance to associate with subsequent IPv4 address family configuration mode commands.

Command Default

IPv6 address prefixes are not enabled. Unicast address prefixes are the default when IPv6 address prefixes are configured.

Note Routing information for address family IPv4 is advertised by default for each BGP routing session configured with the **neighbor remote-as** command unless you configure the **no bgp default ipv4-unicast** command before configuring the **neighbor remote-as** command.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `address-family ipv6` command.

Examples

The following example places the router in address family configuration mode and specifies unicast address prefixes for the IPv6 address family:

```
Router(config)# router bgp 100
Router(config-router)# address-family ipv6 unicast
Router(config-router-af)#
```

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**] [**summary-only**]
no aggregate-address *address mask* [**as-set**] [**summary-only**]

Syntax Description

address	Aggregate address.
mask	Aggregate mask.
as-set	(Optional) Generates autonomous system set path information.
summary-only	(Optional) Filters all more-specific routes from updates.

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)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `aggregate-address` command.

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. Because the **summary-only** keyword is configured, more-specific routes are filtered from updates.

```
router bgp 50000
 aggregate-address 192.168.51.0 255.255.255.0 as-set summary-only
```

bandwidth (policy-map class)

To specify or modify the bandwidth allocated for a class belonging to a policy map, or to enable ATM overhead accounting, use the **bandwidth** command in QoS policy-map class configuration mode. To remove the bandwidth specified for a class or disable ATM overhead accounting, use the **no** form of this command.

bandwidth [**remaining**] **percent** *percentage*
no bandwidth

Syntax Description

remaining	(Optional) Specifies that the percentage of guaranteed bandwidth is based on a relative percent of available bandwidth.
percent *percentage*	Specifies the percentage of guaranteed bandwidth based on an absolute percent of available bandwidth to be set aside for the priority class or on a relative percent of available bandwidth. The valid range is 1 to 100.

Command Default

No bandwidth is specified.

Command Modes

QoS policy-map class configuration (config-pmap-c)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

For usage guidelines, see the Cisco IOS XE `bandwidth (policy-map class)` command.

Examples

The following example shows how to create two policy maps called “PMap” and "generic-cos" and configure two class policies in each policy map.

```
policy-map PMap
 class PMap-super-fast
  priority level 1
  police percent 5
 !
 class PMap-fast
  priority level 2
  police percent 5
 !
!
policy-map generic-cos
 class cos-map-generic
  bandwidth remaining percent 5
  queue-limit 108 packets
 !
 class class-default
  bandwidth remaining percent 95
  queue-limit 2028 packets
 !
!
```

bgp always-compare-med

To enable the comparison of the Multi Exit Discriminator (MED) for paths from neighbors in different autonomous systems, use the **bgp always-compare-med** command in router configuration mode. To disallow the comparison, use the **no** form of this command.

bgp always-compare-med
no bgp always-compare-med

Syntax Description

This command has no arguments or keywords.

Command Default

The software does not compare the MED for paths from neighbors in different autonomous systems if this command is not enabled or if the **no** form of this command is entered. The MED is compared only if the autonomous system path for the compared routes is identical.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `bgp always-compare-med` command.

Examples

In the following example, the local BGP routing process is configured to compare the MED from alternative paths, regardless of the autonomous system from which the paths are received:

```
router bgp 1
 bgp always-compare-med
```

bgp bestpath as-path multipath-relax

To configure a Border Gateway Protocol (BGP) routing process to consider the different autonomous system (AS) paths and load balance multiple paths during best path route selection, use the **bgp bestpath as-path multipath-relax** command in router BGP configuration mode. To return the BGP routing process to the default operation, use the **no** form of this command.

bgp bestpath as-path multipath-relax

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Router BGP configuration (config-router)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	Qualified for use in Cisco vManage CLI templates.

Usage Guidelines

When BGP multi-pathing is enabled, BGP load-balances user traffic within a single autonomous system (AS). The criteria are that all attributes must match (weight, AS path, etc). However, when a device is multi-homed to multiple autonomous systems, BGP cannot load balance traffic between them by default.

In order to enable load-balancing of traffic among the multi-homed autonomous systems, the bgp bestpath as-path multipath-relax command needs to be enabled. The criteria required for this is that the AS-path length should be equal.

Before you use this command, ensure that BGP is enabled.

This command can be used to configure a Border Gateway Protocol (BGP) routing process to consider the different autonomous system (AS) paths and load balance multiple paths during best path route selection.

Example

The following example shows how to configure Border Gateway Protocol (BGP) routing process 65001 to consider the different autonomous system (AS) paths and load balance multiple paths during best path route selection.

```
Router(config)# router bgp 65001
Router(config-router)# bgp bestpath as-path multipath-relax
```

bgp bestpath compare-routerid

To configure a Border Gateway Protocol (BGP) routing process to compare identical routes received from different external peers during the best path selection process and to select the route with the lowest router ID as the best path, use the **bgp bestpath compare-routerid** command in router configuration mode. To return the BGP routing process to the default operation, use the **no** form of this command.

bgp bestpath compare-routerid
no bgp bestpath compare-routerid

Syntax Description

This command has no arguments or keywords.

Command Default

The behavior of this command is disabled by default; BGP selects the route that was received first when two routes with identical attributes are received.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

The **bgp bestpath compare-routerid** command is used to configure a BGP routing process to use the router ID as the tie breaker for best path selection when two identical routes are received from two different peers (all the attributes are the same except for the router ID). When this command is enabled, the lowest router ID will be selected as the best path when all other attributes are equal.

Examples

In the following example, the BGP routing process is configured to compare and use the router ID as a tie breaker for best path selection when identical paths are received from different peers:

```
router bgp 50000
 bgp bestpath compare-routerid
```

bgp bestpath med missing-as-worst

To configure a Border Gateway Protocol (BGP) routing process to assign a value of infinity to routes that are missing the Multi Exit Discriminator (MED) attribute (making the path without a MED value the least desirable path), use the **bgp bestpath med missing-as-worst** command in router configuration mode. To return the router to the default behavior (assign a value of 0 to the missing MED), use the **no** form of this command.

bgp bestpath med missing-as-worst
no bgp bestpath med missing-as-worst

Syntax Description

This command has no arguments or keywords.

Command Default

The software assigns a value of 0 to routes the are missing the MED attribute, causing the route with the missing MED attribute to be considered the best path.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Examples

In the following example, the BGP router process is configured to consider a route with a missing MED attribute as having a value of infinity (4294967294), making this path the least desirable path:

```
router bgp 50000
 bgp bestpath med missing-as-worst
```

bgp deterministic-med

To enforce the deterministic comparison of the Multi Exit Discriminator (MED) value between all paths received from within the same autonomous system, use the **bgp deterministic-med** command in router configuration mode. To disable the required MED comparison, use the **no** form of this command.

bgp deterministic-med
no bgp deterministic-med

Syntax Description

This command has no arguments or keywords.

Command Default

The software does not enforce the deterministic comparison of the MED variable between all paths received from the same autonomous system.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Examples

In the following example, BGP is configured to compare the MED during path selection for routes advertised by the same subautonomous system within a confederation:

```
outer bgp 50000
 bgp deterministic-med
```

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
no bgp graceful-restart

Command Default

By default, the restart time is set to 120 seconds and the stalepath time to 360 seconds.

Command Modes

Address-family configuration (config-router-af)

Router configuration (config-router)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `bgp graceful-restart` command.

Examples

In the following example, the BGP graceful restart capability is enabled for AS number 64496 and disabled for the neighbor:

```
router bgp 64496
 neighbor 10.0.0.1 remote-as 64496
 bgp graceful-restart
 neighbor 10.0.0.1 ha-mode graceful-restart disable
```

bgp log-neighbor-changes

To enable logging of BGP neighbor resets, use the **bgp log-neighbor-changes** command in router configuration mode. To disable the logging of changes in BGP neighbor adjacencies, use the **no** form of this command.

bgp log-neighbor-changes

no bgp log-neighbor-changes

Syntax Description

This command has no arguments or keywords.

Command Default

Logging of BGP neighbor resets is not enabled.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `bgp log-neighbor-changes` command.

Examples

The following example logs neighbor changes for BGP in router configuration mode:

```
bgp router 40000
 bgp log-neighbor-changes
```

bandwidth remaining ratio

To specify a bandwidth-remaining ratio for class-level or subinterface-level queues to be used during congestion to determine the amount of excess bandwidth (unused by priority traffic) to allocate to nonpriority queues, use the **bandwidth remaining ratio** command in policy-map class configuration mode. To remove the bandwidth remaining ratio, use the **no** form of this command.

bandwidth remaining ratio *ratio*
no bandwidth remaining ratio *ratio*

Syntax Description

ratio	Relative weight of this subinterface or class queue with respect to other subinterfaces or class queues. Valid values are from 1 to 1000. At the subinterface level, the default value is platform dependent. At the class queue level, the default is 1.
ratio	Relative weight of this subinterface or class queue with respect to other subinterfaces or class queues.

Command Default

The default bandwidth ratio is 1.

Command Modes

Policy-map class (config-pmap-c)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `bandwidth remaining ratio` command.

Examples

```
class Queue1
   bandwidth remaining ratio 20
   random-detect precedence-based
  !
```

class (policy-map)

To specify the name of the class whose policy you want to create or change or to specify the default class (commonly known as the class-default class) before you configure its policy, use the **class**command in policy-map configuration mode. To remove a class from the policy map, use the **no** form of this command.

class { *class-name* | **class-default** }
no class { *class-name* | **class-default** }

Syntax Description

class-name	Name of the class to be configured or whose policy is to be modified. The class name is used for both the class map and to configure a policy for the class in the policy map.
class-default	Specifies the default class so that you can configure or modify its policy.

Command Default

No class is specified.

Command Modes

Policy-map configuration (config-pmap)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `class (policy-map)` command.

Examples

The following example shows how to create two policy maps called “PMap” and "generic-cos" and configure two class policies in each policy map.

```
policy-map PMap
 class PMap-super-fast
  priority level 1
  police percent 5
 !
 class PMap-fast
  priority level 2
  police percent 5
 !
!
policy-map generic-cos
 class cos-map-generic
  bandwidth remaining percent 5
  queue-limit 108 packets
 !
 class class-default
  bandwidth remaining percent 95
```

```
  queue-limit 2028 packets
 !
!
```

distance bgp

To configure the administrative distance for BGP routes, use the **distance bgp** command in address family or router configuration mode. To return to the administrative distance to the default value, use the **no** form of this command.

distance bgp *external-distance internal-distance local-distance*
no distance bgp

Syntax Description

external-distance	Administrative distance for external BGP routes. Routes are external when learned from an external autonomous system. The range of values for this argument are from 1 to 255.
internal-distance	Administrative distance for internal BGP routes. Routes are internal when learned from peer in the local autonomous system. The range of values for this argument are from 1 to 255.
local-distance	Administrative distance for local BGP routes. Local routes are those networks listed with a **network** router configuration command, often as back doors, for the router or for the networks that is being redistributed from another process. The range of values for this argument are from 1 to 255.

Command Default

The following values are used if this command is not configured or if the no form is entered:

external-distance : 20 *internal-distance*: 200 *local-distance: 200*

Routes with a distance of 255 are not installed in the routing table.

Command Modes

Router configuration (config-router)

Address family configuration (config-router-af)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Starting from this release, this command can be configured in address-family (non-VRF) configuration mode only. It is no longer supported under router configuration mode.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `distance bgp` command.

Examples

The following example is applicable to releases before Cisco IOS XE Catalyst SD-WAN Release 17.2.1v.

In this example, the external distance is set to 10, the internal distance is set to 50, and the local distance is set to 100:

```
router bgp 50000
  distance bgp 10 50 100
  address family ipv4
   network 10.108.0.0
   neighbor 192.168.6.6 remote-as 123
   neighbor 172.16.1.1 remote-as 47
```

The following example is applicable to Cisco IOS XE Catalyst SD-WAN Release 17.4.1a and later.

```
router bgp 50000
 address family ipv4
  network 10.108.0.0
  neighbor 192.168.6.6 remote-as 123
  neighbor 172.16.1.1 remote-as 47
  distance bgp 10 50 100
```

exit-address-family (bgp)

To exit the BGP address family configuration mode, use the **exit-address-family** command in BGP Address-family configuration mode. There is no **no** form of this command.

exit-address-family

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Address-family configuration (config-router-af)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

Cisco routers can use various IP routing protocols, such as Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP), or Border Gateway Protocol (BGP) to learn routes dynamically. You can configure these routing protocols on your router by entering the router configuration mode and address family configuration mode. You can use this command to exit the BGP address family configuration mode.

Example

The following example shows exiting from the BGP address family configuration mode.

```
Router(config)# router bgp 65001
Router(config-router)# address-family ipv4
```

```
Router(config-router-af)# exit-address-family
```

maximum-paths eibgp

To enable multipath load sharing among external Border Gateway Protocol (eBGP) and internal BGP (iBGP) routes, use the **maximum-paths eibgp** command in address family configuration mode. To disable multipath load sharing for eBGP and iBGP routes, use the **no** form of this command.

maximum-paths eibgp *number-of-paths*
no maximum-paths eibgp *number-of-paths*

Syntax Description

number-of-paths	Number of routes to install into the routing table. See the "Usage Guidelines" section for the number of paths that can be configured with this argument.

Command Default

BGP, by default, will install only one best path in the routing table.

Command Modes

Address family configuration (config-router-af)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `maximum-paths eibgp` command.

Examples

The following example shows how to configure this command on a non-VRF address family.

```
Device(config)# router bgp 64498
Device(config-router)# address-family ipv4 unicast
Device(config-router-af)# maximum-paths eibgp 4
```

neighbor advertise-map

To advertise the routes in the BGP table matching the configured route-map, use the **neighbor advertise-map** command in router configuration mode. To disable route advertisement, use the **no** form of this command.

neighbor { *ipv4-address* | *ipv6-address* } **advertise-map** *map-name* { **non-exist-map** *map-name* }
no neighbor { *ipv4-address* | *ipv6-address* } **advertise-map** *map-name* { **non-exist-map** *map-name* }

Syntax Description

ip-address	Specifies the IPv4 address of the router that should receive conditional advertisements.

ipv6-address	Specifies the IPv6 address of the router that should receive conditional advertisements.
advertise-map *map-name*	Specifies the name of the route map that will be advertised if the conditions of the exist map or non-exist map are met.
non-exist-map *map-name*	Specifies the name of the non-exist-map that is compared with the routes in the BGP table to determine whether the advertise-map route is advertised or not.

Command Default

No default behavior or values.

Command Modes

Address family configuration (config-router-af)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `neighbor advertise-map` command.

Examples

The following address family configuration example configures BGP to conditionally advertise a prefix to the 10.1.1.1 neighbor using a non-exist map. If the prefix exists in MAP3 but not MAP4, the condition is met and the prefix is advertised.

```
router bgp 5
 address-family ipv4 unicast
  neighbor 10.1.1.1 advertise-map MAP3 non-exist-map MAP4
```

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* **advertisement-interval** *seconds*
no neighbor *ip-address* **advertisement-interval** *seconds*

Syntax Description

ip-address	IP address of the neighbor.
seconds	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)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

When the MRAI is equal to 0 seconds, BGP routing updates are sent as soon as the BGP routing table changes.

Examples

The following router configuration mode example sets the minimum time between sending BGP routing updates to 600 seconds:

```
router bgp 5
 neighbor 10.0.0.1 advertisement-interval 600
```

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* **description** *text*
no neighbor *ip-address* **description** [*text*]

Syntax Description

ip-address	IP address of the neighbor.
text	Text (up to 80 characters in length) that describes the neighbor.

Command Default

There is no description of the neighbor.

Command Modes

Router configuration (config-router)

Address family configuration (config-router-af)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	This command was introduced.

Examples

In the following examples, the description of the neighbor is “peer with example.com”:

```
router bgp 109
 neighbor 172.16.2.3 description peer with example.com
```

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* } **ebgp-multihop** [*ttl*]
no neighbor { *ip-address* | *ipv6-address* } **ebgp-multihop**

Syntax Description

ip-address	IP address of the BGP-speaking neighbor.
ipv6-address	IPv6 address of the BGP-speaking neighbor.
peer-group-name	Name of a BGP peer group.
ttl	(Optional) Time-to-live in the range from 1 to 255 hops. For Cisco IOS XE Catalyst SD-WAN Release 17.4.1a and later, the supported range is from 2 to 255. If you have configured the value of 1, you must modify the device CLI template or CLI Add-on feature template with supported values.

Command Default

Only directly connected neighbors are allowed.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	This command was introduced.
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	This command was modified. The supported time-to-live range for **ebgp-multihop** is now 2 to 255.

Usage Guidelines

This feature should be used only under the guidance of Cisco technical support staff.

If you specify a BGP peer group by using the *peer-group-name* argument, all the members of the peer group will inherit the characteristic configured with this command.

To prevent the creation of loops through oscillating routes, the multihop will not be established if the only route to the multihop peer is the default route (0.0.0.0).

Examples

The following example allows connections to or from neighbor 10.108.1.1, which resides on a network that is not directly connected:

```
router bgp 109
 neighbor 10.108.1.1 ebgp-multihop 255
```

neighbor ha-mode graceful-restart

To enable or disable the Border Gateway Protocol (BGP) graceful restart capability for a BGP neighbor or peer group, use the **neighbor ha-mode graceful-restart** command in router configuration mode. To remove from the configuration the BGP graceful restart capability for a neighbor, use the **no** form of this command.

neighbor *ip-address* **ha-mode graceful-restart** [**disable**]
no neighbor *ip-address* **ha-mode graceful-restart** [**disable**]

Syntax Description

ip-address	IP address of the neighbor.
disable	(Optional) Disables BGP graceful restart capability for a neighbor.

Command Default

BGP graceful restart capability is disabled.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `neighbor ha-mode graceful-restart` command.

Examples

The following example enables the BGP graceful restart capability for the BGP neighbor, 172.21.1.2:

```
router bgp 45000
 bgp log-neighbor-changes
 address-family ipv4 unicast
 neighbor 172.21.1.2 remote-as 45000
 neighbor 172.21.1.2 activate
 neighbor 172.21.1.2 ha-mode graceful-restart
 end
```

The following example enables the BGP graceful restart capability globally for all BGP neighbors and then disables the BGP graceful restart capability for the BGP neighbor 10.0.0.1.

```
router bgp 64496
 neighbor 10.0.0.1 remote-as 64496
 bgp graceful-restart
 neighbor 10.0.0.1 ha-mode graceful-restart disable
```

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*]
no neighbor *ip-address* **maximum-prefix** *maximum*

Syntax Description

ip-address	IP address of the neighbor.
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 *maximum*-prefix 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 maximum-prefix limit has been exceeded. The restart timer is configured with the *restart-interval* argument.
restart-interval	(Optional) Time interval (in minutes) that a peering session is reestablished. The range is from 1 to 65535 minutes.

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

Address family configuration (config-router-af)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `neighbor maximum-prefix (BGP)` command.

Examples

In the following example, the maximum number of prefixes that will be accepted from the 192.168.3.3 neighbor is set to 769434. The router is configured to display a warning when 100 percent of the prefixes is reached. The router is also configured to reestablish a disabled peering session after 65535 minutes.

```
router bgp 40000
 address-family ipv4 unicast
  neighbor 192.168.3.3 maximum-prefix 769434 100 restart 65535
```

neighbor next-hop-self

To configure a router as the next hop for a BGP-speaking neighbor or peer group, use the **neighbor next-hop-self** command in router configuration mode. To disable this feature, use the **no** form of this command.

neighbor *ip-address* **next-hop-self**

no neighbor *ip-address* **next-hop-self**

Syntax Description

ip-address	IP address of the BGP-speaking neighbor.

Command Default

This command is disabled by default.

Command Modes

Address family configuration (config-router-af)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `neighbor next-hop-self` command.

Examples

The following example forces all updates destined for 10.108.1.1 to advertise this router as the next hop:

```
router bgp 109
 neighbor 10.108.1.1 next-hop-self
```

neighbor password

To enable message digest5 (MD5) authentication on a TCP connection between two BGP peers, use the **neighbor password** command in router configuration mode. To disable this function, use the **no** form of this command.

neighbor *ip-address* **password** [*type*] *string*
no neighbor *ip-address* **password**

Syntax Description

ip-address	IP address of the BGP-speaking neighbor.
peer-group-name	Name of a BGP peer group.
type	(Optional) The type of password. You can only specify the following: • *0*: Unencrypted • *7*: Encrypted with MD5 Even though the CLI accepts other values only these value change the encryption of the password.
string	Case-sensitive password of up to 25 characters in length. The first character cannot be a number. The string can contain any alphanumeric characters, including spaces. You cannot specify a password in the format *number-space-anything*. The space after the number can cause authentication to fail.

Command Default

MD5 is not authenticated on a TCP connection between two BGP peers.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `neighbor password` command.

Examples

The following example configures MD5 authentication for the peering session with the 10.108.1.1 neighbor. The same password must be configured on the remote peer before the hold-down timer expires.

```
router bgp 109
 neighbor 10.108.1.1 password 7 00141215174C04140B1E1E
```

neighbor remote-as

To add an entry to the BGP or multiprotocol BGP neighbor table, use the **neighbor remote-as** command in router configuration mode. To remove an entry from the table, use the **no** form of this command.

neighbor { *ip-address* | *ipv6-address* } **remote-as** *autonomous-system-number*
no neighbor { *ip-address* | *ipv6-address* } **remote-as** *autonomous-system-number*

Syntax Description

ip-address	IP address of the neighbor.
ipv6-address	IPv6 address of the neighbor.
autonomous-system-number	Number of an autonomous system to which the neighbor belongs in the range from 1 to 65535.

Command Default

There are no BGP or multiprotocol BGP neighbor peers.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `neighbor remote-as` command.

Examples

The following example specifies that a router at the address 10.0.0.1 is an internal BGP (iBGP) neighbor in autonomous system number 64496:

```
router bgp 64496
 neighbor 10.0.0.1 remote-as 64496
 bgp graceful-restart
 neighbor 10.0.0.1 ha-mode graceful-restart disable
```

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* | *ipv6-address* [**%**] } **route-map** *map-name* { **in** | **out** }
no neighbor { *ip-address* | *ipv6-address* [**%**] } **route-map** *map-name* { **in** | **out** }

Syntax Description

ip-address	IP address of the neighbor.
ipv6-address	IPv6 address of the neighbor.
%	(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.
map-name	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

Address family configuration (config-router-af)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `neighbor route-map` command.

Examples

The following address family configuration mode example applies a route map named internal-map to a unicast BGP route from 172.16.70.24:

```
router bgp 5
address-family ipv4 unicast
 neighbor 172.16.70.24 route-map internal-map in
```

neighbor send-community

To specify that a communities attribute should be sent to a BGP neighbor, use the **neighbor send-community** command in address family or router configuration mode. To remove the entry, use the **no** form of this command.

neighbor { *ip-address* *ipv6-address* } **send-community** **both**
no **neighbor** *ip-address ipv6-address* **send-community**

Syntax Description

ip-address	IP address of the neighbor.
ipv6-address	IPv6 address of the neighbor.
both	(Optional) Specifies that both standard and extended communities will be sent.

Command Default

No communities attribute is sent to any neighbor.

Command Modes

Address family configuration (config-router-af)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Examples

In the following address family configuration mode example, the router belongs to autonomous system 109 and is configured to send the communities attribute to its neighbor at IP address 172.16.70.23:

```
router bgp 109
 address-family ipv4 unicast
  neighbor 172.16.70.23 send-community both
```

neighbor shutdown

To disable a neighbor or peer group or to gracefully shut down a link for maintenance, use the **neighbor shutdown** command in router configuration mode or address family configuration mode. To reenable the neighbor or peer group, use the **no** form of this command.

neighbor *ip-address* **shutdown**
no **neighbor** *ip-address* **shutdown**

Syntax Description

ip-address	IP address of the neighbor.

Command Default

No change is made to the status of any BGP neighbor or peer group.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `neighbor shutdown` command.

Examples

The following example disables any active session for the neighbor 172.16.70.23:

```
router bgp 123134
 neighbor 172.16.70.23 shutdown
```

neighbor timers

To set the timers for a specific BGP peer or peer group, use the **neighbor timers** command in address family or router configuration mode. To clear the timers for a specific BGP peer or peer group, use the **no** form of this command.

neighbor *ip-address* **timers** *keepalive holdtime*
no neighbor *ip-address* **timers**

Syntax Description

ip-address	(Optional) A BGP peer or peer group IP address.
keepalive	Frequency (in seconds) with which the Cisco IOS software sends *keepalive* messages to its peer. The default is 60 seconds.The range is from 0 to 65535.
holdtime	Interval (in seconds) after not receiving a *keepalive* message that the software declares a peer dead. The default is 180 seconds. The range is from 0 to 65535.

Command Default

keepalive : 60 seconds*holdtime*: 180 seconds

Command Modes

Router configuration (config-router)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `neighbor timers` command.

Examples

The following example changes the keepalive timer to 70 seconds and the hold-time timer to 210 seconds for the BGP peer 192.168.47.0:

```
router bgp 109
 neighbor 192.168.47.0 timers 70 210
```

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*] }
no network { *network-number* [**mask** *network-mask*] }

Syntax Description

network-number	Network that BGP will advertise.
mask *network-mask*	(Optional) Network or subnetwork mask with mask address.

Command Default

No networks are specified.

Command Modes

Address family configuration (config-router-af)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

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 192.168.51.0 with mask of 255.255.255.0 to be included in unicast BGP updates:

```
router bgp 64800
 address-family ipv4 unicast
  network 192.168.51.0 mask 255.255.255.0
```

police (percent)

To configure traffic policing on the basis of a percentage of bandwidth available on an interface, use the **police** command in policy-map class configuration mode. To remove traffic policing from the configuration, use the **no** form of this command.

police rate percent *percentage*
no police rate percent *percentage*

Syntax Description

rate	Specifies the information rate.
percent	Specifies that a percentage of bandwidth will be used for calculating the CIR.

percentage	The bandwidth percentage. Valid range is a number from 1 to 100.

Command Default

No traffic policing is configured.

Command Modes

Policy-map class configuration (config-pmap-c)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `police (percent)` command.

Examples

The following example shows how to configure traffic policing:

```
Policy-map PMap
 class PMap-super-fast
  priority level 1
  police rate percent 5
 class PMap-fast
  priority level 2
  police rate percent 5
 !
!
policy-map generic-cos
 class cos-map-generic
  bandwidth remaining percent 5
  queue-limit 108 packets
 class class-default
  bandwidth remaining percent 95
  queue-limit 2028 packets
```

policy-map

To enter policy-map configuration mode and create or modify a policy map that can be attached to one or more interfaces to specify a service policy, use the **policy-map**command in global configuration mode. To delete a policy map, use the **no** form of this command.

policy-map [**type inspect**] *policy-map-name*
no policy-map [**type inspect**] *policy-map-name*

Syntax Description

type inspect	(Optional) Specifies the policy-map type as inspect.
policy-map-name	Name of the policy map.

Command Default

The policy map is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Qualified for use in Cisco vManage CLI templates.
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	Command modified to support **type inspect**.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `policy-map` command.

Examples

The following example shows how to create two policy maps called “PMap” and "generic-cos" and configure two class policies in each policy map.

```
policy-map PMap
 class PMap-super-fast
  priority level 1
  police percent 5
 !
 class PMap-fast
  priority level 2
  police percent 5
 !
!
policy-map generic-cos
 class cos-map-generic
  bandwidth remaining percent 5
  queue-limit 108 packets
 !
 class class-default
  bandwidth remaining percent 95
  queue-limit 2028 packets
 !
!
```

priority level

To configure multiple priority queues, use the **priority level** command in policy-map class configuration mode. To remove a previously specified priority level for a class, use the **no** form of this command.

priority level *level*
no priority level *level*

Syntax Description

level	Defines multiple levels of a strict priority service model. When you enable a traffic class with a specific level of priority service, the implication is a single priority queue associated with all traffic that is enabled with the specified level of priority service. Valid values are from 1 (high priority) to 2 (low priority). Default is 1.

Command Default

The priority level has a default level of 1.

Command Modes

Policy-map class configuration (config-pmap-c)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `priority level` command.

Examples

The following example shows how to configure multi level priority queues. In the example, the traffic class named PMap-super-fast is given high priority (level 1), and the class named PMap-fast is given level 2 priority. To prevent PMap-fast traffic from becoming starved of bandwidth, PMap-super-fast traffic is policed at 5 percent of the available bandwidth.

```
Policy-map PMap
 class PMap-super-fast
  priority level 1
  police percent 5
 class PMap-fast
  priority level 2
  police percent 5
 !
!
```

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.

redistribute { **omp** | **static** | **connected** | **nat-route** }

no redistribute { **omp** | **static** | **connected** | **nat-route** }

Syntax Description

omp	The omp keyword specifies OMP as the source protocol from which routes are being redistributed.].
static	The **static** [**ip**] keyword is used to redistribute IP static routes.
connected	The **connected** keyword refers to routes that are established automatically by virtue of having enabled IP on an interface.
nat-route	The **nat-route** keyword redistributes NAT66 DIA routes into BGP protocol.

Command Default

Route redistribution is disabled.

Command Modes

Address family configuration (config-af)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	Command qualified for use in Cisco vManage CLI templates.
Cisco IOS XE Catalyst SD-WAN Release 17.14.x	This command was modified. Added the **nat-route** keyword to redistribute NAT66 DIA routes into BGP protocol.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `redistribute` (IP) command.

Examples

The following example redistributes a NAT66 DIA route into BGP:

```
router bgp 15
bgp bestpath as-path multipath-relax
bgp log-neighbor-changes
bgp router-id 10.1.1.1
address-family ipv4 unicast vrf 1
 neighbor 10.2.2.2 remote-as 2
 neighbor 10.2.2.2 activate
 redistribute nat-route dia
 exit-address-family
!
address-family ipv6 unicast vrf 1
 bgp router-id 10.1.1.1
 neighbor 2001:a14:18::64 remote-as 2
 neighbor 2001:a14:18::64 activate
 redistribute nat-route
 exit-address-family
!
```

The following example redistributes a NAT66 DIA route into OSPFv3:

```
interface GigabitEthernet5
ospfv3 1 network point-to-point
ospfv3 1 ipv4 area 0
ospfv3 1 ipv6 area 0
router ospfv3 1
max-lsa 50000
router-id 10.1.1.1
address-family ipv4 unicast vrf 1
 log-adjacency-changes
 redistribute connected
 exit-address-family
!
address-family ipv6 unicast
 log-adjacency-changes
 redistribute connected
 redistribute nat-route
 redistribute maximum-prefix 10240
 exit-address-family
!
```

Examples

The following example redistributes routes for an IPv4 address family:

```
router bgp 64496
 address-family ipv4 unicast vrf 1
  redistribute omp
  redistribute static
```

```
  redistribute connected
  exit-address-family
```

The following example redistributes routes for an IPv6 address family:

```
Device(config)# router eigrp 1
Device(config-router)# address-family ipv6 unicast vrf 1 autonomous-system 3
Device(config-router-af)# topology base
Device(config-router-af-toplogy)# redistribute static route-map route-map1
```

redistribute omp (bgp)

To enable redistributing omp routes into BGP, use the **redistribute omp** command in BGP Address-family IP configuration mode. To disable redistributing omp routes into BGP, use the **no** form of this command.

redistribute omp { **route-map** *string* }

no redistribute omp { **route-map** *string* }

Syntax Description

None	Enable redistributing omp routes into BGP.
route-map*string*	(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.

Command Default

None

Command Modes

BGP Address-family IP configuration (config-router-af)

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

By default, routes from other routing protocols are not redistributed into BGP. It can be useful for BGP to learn OMP routes, because OMP learns routes to destinations throughout the overlay network.

This command can be used to enable redistributing omp routes into BGP.

Example

The following example shows how to enable redistributing omp into BGP process 65001.

```
Router(config)# router bgp 65001
Router(config-router)# address-family ipv4
Router(config-router-af)# redistribute omp
```

The following example shows how to enable redistributing omp with the route-map named OMP-to-BGP into BGP process 65001.

```
Router(config)# router bgp 65001
Router(config-router)# address-family ipv4
Router(config-router-af)# redistribute omp route-map OMP-to-BGP
```

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

autonomous-system-number	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 for 2-byte non asdot notation. 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. **Note** When you run this command, the Cisco SD-WAN device does not verify the accuracy of the entered values. However when you commit the CLI, any invalid CLIs, either syntax or functionality, are rejected.

Command Default

No BGP routing process is enabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	Qualified for use in Cisco vManage CLI templates. with an *autonomous-system-number* of 64496.
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command modified to include full range of *autonomous-system-number*s

Usage Guidelines

For further usage guidelines on this command, see the Cisco IOS XE router bgp command.

Examples

Examples:

```
router bgp 64496
 neighbor 10.0.0.1 remote-as 64496
 bgp graceful-restart
 neighbor 10.0.0.1 ha-mode graceful-restart disable
```

```
router bgp 64496
 address-family ipv4 unicast vrf 1
 redistribute omp
 redistribute static
 redistribute connected
```

timers bgp

To adjust BGP network timers, use the **timers bgp** command in router configuration mode. To reset the BGP timing defaults, use the **no** form of this command.

timers bgp *keepalive holdtime* [*min-holdtime*]
no timers bgp

Syntax Description

keepalive	Frequency (in seconds) with which the Cisco IOS software sends *keepalive* messages to its peer. The default is 60 seconds. The range is from 0 to 65535.
holdtime	Interval (in seconds) after not receiving a *keepalive* message that the software declares a peer dead. The default is 180 seconds. The range is from 0 to 65535.
min-holdtime	(Optional) Interval (in seconds) specifying the minimum acceptable hold-time from a BGP neighbor. The minimum acceptable hold-time must be less than, or equal to, the interval specified in the *holdtime*argument. The range is from 0 to 65535.

Command Default

keepalive : 60 seconds

holdtime: 180 seconds

Command Modes

Router configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

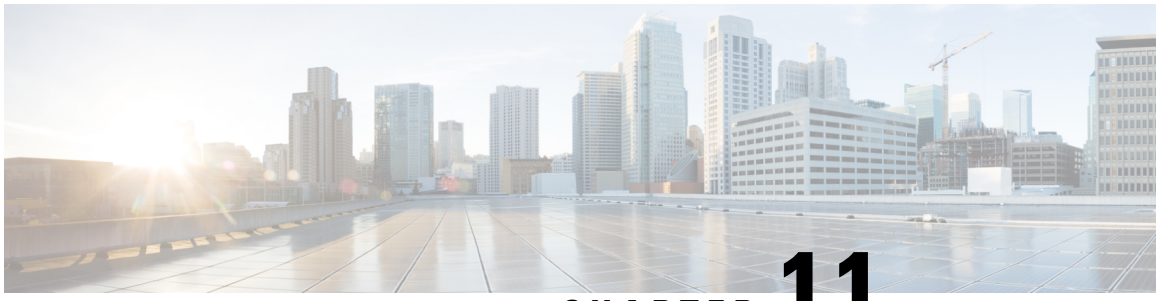
Usage Guidelines

For usage guidelines, see the Cisco IOS XE `timers bgp` command.

Examples

The following example changes the keepalive timer to 70 seconds, the hold-time timer to 130 seconds, and the minimum acceptable hold-time interval to 100 seconds:

```
router bgp 45000
 timers bgp 70 130 100
```



CHAPTER 11

Cellular Commands

- lte gps (cellular), on page 123
- lte sim, on page 125
- profile id, on page 125
- lte gps constellation, on page 127
- lte modem crash-action, on page 127
- lte profile reset, on page 128
- lte modem dm-log, on page 129
- lte450 profile, on page 130
- lte450 credential, on page 132
- lte450 band, on page 133

lte gps (cellular)

To configure Global Positioning System (GPS) parameters for a cellular router, use the **lte gps** command in cellular configuration mode. To delete the GPS configuration parameters, use the no form of this command.

lte gps { **mode** { **ms-based** | **standalone** } [**enable**] [**nmea** [**ip udp** *ipv4-address*]] | **enable** [**mode** { **ms-based** | **standalone** }] [**nmea** [**ip udp** *ipv4-address*]] | **nmea** [**ip udp** *source-ip-address destination-ip-address port*] }

no lte gps

Syntax Description

lte gps	Enables GPS on the LTE PIM module in the 0/x/0 section of the controller cellular configuration.
mode	Specifies the mode. • **ms-based**: Use mobile station-based assistance, also called assisted GPS mode, when determining position. In this mode, a network data session is used to obtain the GPS satellite locations, resulting in a faster fix of location coordinates. • **standalone**: Use satellite information when determining position. **Note** The **standalone** parameter is currently not supported for geofencing.

ms-based	Enables ms-based assistance. **Note** We recommend using **ms-based** mode with a SIM card plugged in and a GPS antenna connected to the LTE pluggable module GPS port. For more information, see Cisco 4G Indoor/Outdoor Active GPS Antenna (GPS-ACT-ANTM-SMA).
standalone	Enables **standalone** mode. If there is no SIM card inserted, you can use **standalone** mode. **Note** The **standalone** parameter is currently not supported for geofencing.
enable	Enables the GPS features. Use this command to enable the GPS feature if GPS has been disabled for any reason.
nmea	Enables the use of National Marine Electronics Association (NMEA) streams to Cisco IOS applications for listening to the specified port on the destination address.
ip	(Optional) Enables the redirection of GPS NMEA streams to the destination IP address. **Note** This parameter is not used for configuring geofencing.
udp *source-ip-address destination-ip-address port*	(Optional) Enables the redirection of GPS NMEA streams to the source and destination IP address and port. **Note** This parameter is not used for configuring geofencing.

Command Modes

controller Cellular 0/x/0 (config-Cellular-0/x/0)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

If multiple LTE pluggable module slots are present in the platform chassis, we recommend that you configure GPS on only one of the LTE pluggable module slots and use the slot for GPS coverage.

Examples

The following example enables GPS on the LTE PIM module:

```
Device(config)# controller Cellular 0/2/0
Device(config-Cellular-0/2/0)# lte gps enable
```

The following example sets ms-based assistance on the LTE PIM module:

```
Device(config-Cellular-0/2/0)# lte gps mode ms-based
```

The following example configures nmea on the LTE PIM module:

```
Device(config-Cellular-0/2/0)# lte gps nmea
```

lte sim

To configure Subscriber Identity Module (SIM) parameters for a cellular router, use the **lte sim** command in cellular configuration mode. To delete the SIM configuration parameters, use the no form of this command.

lte sim [**attach-profile** *attach-profile* **data-profile** *data-profile* **slot** *slot*]

no lte sim

Syntax Description

lte sim	Enables SIM on the LTE cellular module in the 0/x/0 section of the controller cellular configuration.
attach-profile	Attaches the profile on the LTE PIM module in the 0/x/0 section of the controller cellular configuration.
data-profile	Default profile on the LTE PIM module in the 0/x/0 section of the controller cellular configuration.
slot	SIM slot that contains the SIM to configure. Valid values are 0 (primary SIM card) and 1 (secondary SIM card).

Command Modes

controller Cellular 0/x/0 (config-Cellular-0/x/0)

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Dual Subscriber Identity Module (SIM) provides reliability and multihoming capabilities over LTE and HSPA-based networks. With two LTE modems, the IR829 enables concurrent connectivity to two cellular networks for high reliability, enhanced data throughputs, load balancing and differentiated services.

Example

The following example enables SIM on the LTE SIM module:

Examples

```
Device(config)# controller Cellular 0/2/0
Device(config-Cellular-0/2/0)# lte sim enable
Device(config-Cellular-0/2/0)# lte sim attach-profile 1 data-profile 1 slot 0
```

profile id

To create a data profile for a device, use the **profile id** command in cellular configuration mode. To set the command to the default state, use the **no** form of this command.

profile id *id* **apn** *name* [**authentication** *auth_type* **username** *username* **password** *password*] [**pdn-type** *pdn_type*] [**slot** *slot_number*]

no profile id *id*

Syntax Description

id	Identification number of the data profile. Valid values are from 1 to 16.
apn *name*	Name of the access point network of the service provider.
authentication *auth_type*	Authentication type used for APN access. Valid values are: • **chap**: Use CHAP authentication only. • **pap**: Use PAP authentication only. • **pap_chap**: Use PAP or CHAP authentication.
username *username*	Username provided by the service provider for APN access authentication. Required if the authentication type is **chap**, **pap**, or **pap_chap**, otherwise not used.
password *password*	Password provided by the service provider for APN access authentication. Required if the authentication type is **chap**, **pap**, or **pap_chap**, otherwise not used.
pdn-type *pdn_type*	Type of packet data matching used for APN access. Valid values are: • **ipv4**: IPv4 type bearer. • **ipv4v6**: IPV4V6 type bearer. • **ipv6**: IPv6 type bearer.
slot-number *slot_number*	SIM slot that contains the SIM to configure. Valid values are 0 (primary SIM card) and 1 (secondary SIM card).

Command Default

By default, when the Auto SIM feature is enabled on a modem, a data profile is selected based on the modem firmware.

Command Modes

Controller cellular configuration (controller-cellular)

Command History

Release	Modification
Cisco SD-WAN Release 20.8.1	This command was introduced.

Usage Guidelines

If a device contains two SIM cards, you can create a separate data profile for each SIM card.

Examples

The following example shows how to configure a data profile for the primary SIM card in a device:

```
controller Cellular 0/1/0
 profile id 6 apn test authentication chap username admin password my_password pdn-type
ipv4 slot 0
```

lte gps constellation

To configure the Global Navigation Satellite System (GNSS) constellations on a Cisco IOS XE Catalyst SD-WAN device, use the **lte gps constellation** command in cellular configuration mode. To disable the GNSS settings, use the **no** form of this command.

lte gps constellation { **beidou** | **galileo** | **glonass** | **gps** | **gnss** }

no lte gps constellation

beidou	Enable **beidou** as an active constellation.
galileo	Enable **galileo** as an active constellation.
glonass	Enable **glonass** as an active constellation.
gps	Enable **gps** as an active constellation.
gnss	Choose **gnss** to enable multiple GNSS constellations.

Command Default

No default behavior or values.

Command Modes

Controller cellular configuration (controller-cellular)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.15.1a	Command qualified for use in Cisco Catalyst SD-WAN Manager CLI templates.

Examples

The following example shows how to configure GNSS constellation on a Cisco IOS XE Catalyst SD-WAN device:

```
Device(config)# controller cellular 0/1/0
Device(config-controller)# lte gps constellation gps
```

lte modem crash-action

To configure the lte-modem crash-action on a Cisco IOS XE Catalyst SD-WAN device, use either of these two commands in cellular configuration mode.

lte modem crash-action {auto-collect|boot-and-hold}

To disable the crash-action auto-collect settings, use this command.

no lte modem crash-action auto-collect

Syntax Description

Table 10:

auto-collect	The modem recovers within one minute and automatically generates crash dump log. When the modem crashes, the modem will go to Boot and Hold mode. The user can detect this mode with this option configured and collect the modem crash dump automatically. When the crash dump is collected, the user can reset the modem, which will go to **online** mode.
boot-and-hold	When the modem crashes, the modem will go to **Boot and Hold** mode. The user has the option to collect the modem crash dump manually. The modem will stay in this mode until modem crash dump is collected.

Command Default

No default behavior or values.

Command Modes

Cellular configuration mode

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.18.1a	The command **lte modem crash-action auto-collect** was introduced.

Example

The following example shows how to configure lte-modem-crash-action in a device:

```
Router(config-controller)#lte modem crash-action ?
  auto-collect   Remain in crash state and auto collect crash dump
  boot-and-hold  Remain in crash stateRouter(config-controller)#lte modem crash-action
auto-collect
```

lte profile reset

To reset the configuration of a cellular modem operating on a Cisco IOS XE Catalyst SD-WAN device, use the **cellular***slot* **lte profile reset** command in cellular configuration mode.

Syntax Description

lte profile reset	Resets the configured modem slot profile to the factory default profile.

Command Default

No default behavior or values.

Command Modes Cellular configuration mode

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.18.1a	The command **cellular***slot* **lte profile reset** was introduced.

Example

The following example shows how to configure **cellular <slot> lte profile reset** in a device:

```
CellularGateway# cellular 0/2/0 profile-reset
```

lte modem dm-log

To configure integrated Diagnostic Monitor (DM) logging to monitor traffic on a modem, use the **lte modem dm-log** command in controller cellular configuration mode.

lte modem dm-log { **enable** | **filesize** *size* | **filter** *location : filename* | **output path** *URL* | **rotation** | **size** *log-size* }

Syntax Description

lte modem	Enables, disables, or modifies the cellular configuration on a LTE PIM module in the 0/*x*/0 section of the controller cellular configuration.
enable	Enables DM logging.
filesize *size*	Specifies the maximum log file size, in MB. Range is from 1 to 64. Default is 20.
filter *location : filename*	Specifies the DM log filter file location and filename. These are the valid values for the *location* parameter: **flash0**, **flash1**, **flash**, **usbflash**, **usbflash0**, or **usbflash1** **Note:** If you do not specify a DM log filter file, the command uses a generic filter file which comes with the diagnostic software tool. **Note:** Supported file format: SQF
output path *URL*	Specifies the location for storing the DM logging output files. The router's flash storage is the default path.
rotation	Enables log rotation. **Note:** The **rotation** option is only supported if you store the log files on the router flash drive or a USB flash drive.
size *log-size*	Maximum log size (MB). Range: 0 to 1024 Default: 64

Command Default No default behavior or values.

Command Modes controller cellular configuration (config-Cellular-0/*x*/0)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines When you modify the dm-log configuration from the CLI or via Cisco SD-WAN Manager, you may see the following message:

```
Log rotation is enabled, please make sure DM logging file size is smaller than 64MB, the
default maximum log size before removing "modem dm-log size" cfg."
```

In such cases, update the `lte modem dm-log filesize` configuration to remove or modify the rest of the dm-log settings. You can achieve this in two ways.

Option 1: Remove the dm-log filesize configuration and then update the rest of the dm-log configurations.

```
Device# config-transaction
admin connected from 10.0.0.1 using console on Device
Device(config)# controller Cellular 0/2/0
Device(config-Cellular-0/2/0)# no lte modem dm-log filesize 64
Device(config-Cellular-0/2/0)# commit
Commit complete.
Device(config-Cellular-0/2/0)# end
Device#
```

Option 2: Update the dm-log filesize configuration to a value less than 64 and then update the rest of the dm-log configurations.

```
Device# config-t
admin connected from 10.0.0.1 using console on Device
Device(config)# controller Cellular 0/2/0
Device(config-Cellular-0/2/0)# lte modem dm-log filesize 25
Device(config-Cellular-0/2/0)# commit
Commit complete.
Device(config-Cellular-0/2/0)# no lte modem dm-log size 1024
Device(config-Cellular-0/2/0)# no lte modem dm-log rotation
Device(config-Cellular-0/2/0)# commit
Commit complete.
Device(config-Cellular-0/2/0)# end
Device# show running-config controller Cellular 0/2/0
Building configuration...
Current configuration : 266 bytes
!
controller Cellular 0/2/0
lte modem dm-log filesize 25
profile id 1 apn internet authentication none pdn-type ipv4
profile id 2 apn embb authentication none pdn-type ipv4 slice-type 1
profile id 3 apn urllc authentication none pdn-type ipv4 slice-type 2
end
```

lte450 profile

To create a profile for a P-LTE-450 module in a device, specifying connection parameters such as profile ID, APN, authentication, PDN type, and VLAN, use the **lte450 profile** command in global configuration mode. To set the command to the default state, use the **no** form of this command.

lte450 profile id *id* **apn** *apn_name* [**authentication** *auth_type* **username** *username* **password** *password*] [**pdn-type** *pdn_type*] [**vlan** *vlan_id*]

no profile id *id*

Syntax Description

id	Identification number of the data profile. Valid values are from 1 to 3.
apn *apn_name*	Name of the access point network of the service provider.
authentication *auth_type*	Authentication type used for APN access. Valid values are: • **chap**: Use CHAP authentication only. • **pap**: Use PAP authentication only. • **none**: Use none authentication.
pdn-type *pdn_type*	Type of packet data matching used for APN access. Valid values are: • **ipv4**: IPv4 type bearer. • **ipv4v6**: IPV4V6 type bearer. • **ipv6**: IPv6 type bearer.
vlan *vlan_id*	Configures VLAN settings for the APN. VLAN ID is the VLAN number. The range is 1 to 4094.

Command Default

No default behavior or values.

Command Modes

Interface configuration (config-if)

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.18.1a	This command was introduced.

Usage Guidelines

- Configure the username and password of the P-LTE-450 module, see **lte450 credential** command.
- Provide an appropriate *apn_name* such as **`internet`**. It should be communicated by your service provider.
- Provide an appropriate *vlan_id* such as **`2`**.

Examples

The following example shows how to configure a profile for P-LTE-450 module in a device:

```
Device(config)#interface GigabitEthernet0/4/0
Device(config-if)#no shutdown
```

```
Device(config-if)#ip address dhcp
Device(config-if)#negotiation auto
Device(config-if)#lte450 credential username admin password VzbhPxZJ42WUhPHB
Device(config-if)#lte450 band 31
Device(config-if)#lte450 profile id 2 apn internet authentication none pdn-type ipv4 vlan
2
Device(config-if)#Exit
Device(config)#interface GigabitEthernet0/4/0.2
Device(config-if)#description LTE450 Interface
Device(config-if)#no shutdown
Device(config-if)#encapsulation dot1Q 2
Device(config-if)#ip address dhcp
```

lte450 credential

To configure authentication credentials for an P-LTE-450 module in a device, use the **lte450 credential** command in global configuration mode. To remove the credentials configuration, use the **no** form of this command.

lte450 credential username *username* **password** *password*

no credential

Syntax Description

username *username*	Username provided by the service provider for APN access authentication. Required if the authentication type is **chap**, **pap**, or **none**. If the authentication type is none, username and password fields will not be required.
password *password*	Password is the password on the sticker label that comes with the P-LTE-450 module.

Command Default

No default behavior or values.

Command Modes

Interface configuration (config-if)

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.18.1a	This command was introduced.

Usage Guidelines

password is the password on the sticker label that comes with the P-LTE-450 module.

Examples

The following example shows how to configure the usename and password for a P-LTE-450 module in a device.

```
Device(config)#interface GigabitEthernet0/4/0
Device(config-if)#no shutdown
Device(config-if)#ip address dhcp
```

```
Device(config-if)#negotiation auto
Device(config-if)#lte450 credential username admin password VzbhPxJ42WUhHB
Device(config-if)#lte450 band 31
Device(config-if)#lte450 profile id 2 apn internet authentication none pdn-type ipv4 vlan
2
Device(config-if)#Exit
```

lte450 band

To configure a band for an LTE 450 MHz module in a device, use the **lte450 band** command in global configuration mode. To delete the credential configuration, use the **no** form of this command.

lte450 band { **31** | **72** }

no band

Syntax Description

lte450 band	Specifies the the modem band.
31	Specifies LTE band 31 (450 MHz).
72	Specifies LTE band 72 (450 MHz).

Command Default

No default behavior or values.

Command Modes

Interface configuration (config-if)

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.18.1a	This command was introduced.

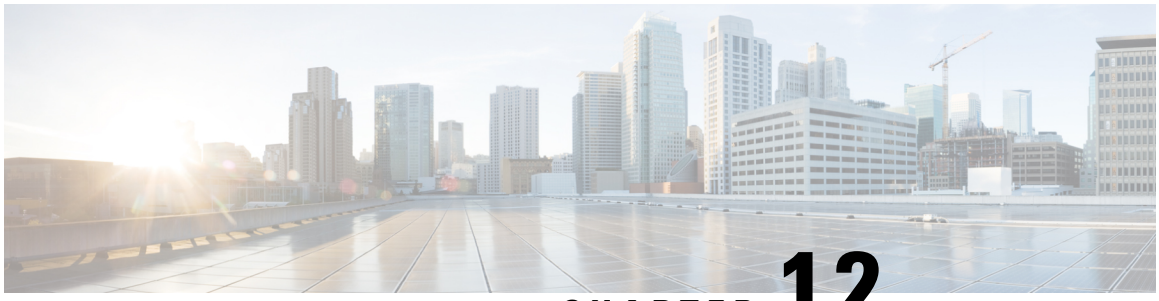
Usage Guidelines

Use **band 31** or **72**.

Examples

The following example shows how to configure the band for P-LTE-450 module in a device:

```
Device(config)#interface GigabitEthernet0/4/0
Device(config-if)#no shutdown
Device(config-if)#ip address dhcp
Device(config-if)#negotiation auto
Device(config-if)#lte450 credential username admin password VzbhPxZJ42WUhPHB
Device(config-if)#lte450 band 31
Device(config-if)#lte450 profile id 2 apn internet authentication none pdn-type ipv4 vlan
2
Device(config-if)#Exit
```



CHAPTER 12

CFM Commands

Note This documentation set includes commands that are tested and verified on a Cisco IOS XE SD-WAN device using the Device Configuration-Based CLI Templates or the CLI add-on feature template.

- alarm, on page 135
- cfm mep domain, on page 136
- cos, on page 137
- ethernet cfm ieee, on page 137
- ethernet cfm global, on page 137
- ethernet oam, on page 138
- ethernet oam remote-loopback, on page 138
- ethernet loopback permit, on page 139
- snmp-server enable traps ethernet cfm cc, on page 139
- snmp-server enable traps ethernet cfm crosscheck, on page 140
- ethernet evc, on page 140
- ethernet cfm domain level, on page 140
- offload sampling, on page 141
- sender-id, on page 142
- service (CFM-srv), on page 143
- service evc, on page 144
- continuity-check, on page 144

alarm

To configure an alarm when fault alarms are enabled, use the **alarm** command in Ethernet connectivity fault management (CFM) interface configuration mode. To remove the configuration, use the **no** form of this command.

notification	Sets the defects that are to be reported if fault alarms are enabled.
all	Reports all defects: DefRDI, DefMACStatus, DefRemote, DefError, and DefXcon.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE alarm command.

Examples

The following example shows how to set up notifications for all defects:

```
Interface interface-name
 cfm mep domain domain-name mpid id service service-name
  alarm notification all
```

cfm mep domain

To configure a maintenance endpoint (MEP) for a domain, use the **cfm mep domain** command in either service instance configuration mode or virtual forwarding instance (VFI) configuration mode. To remove the MEP, use the **no** form of this command.

Syntax Description

domain-name	String from 1 to 154 characters that identifies the domain name.
mpid	Indicates the maintenance point ID (MPID).
mpid-value	Integer from 1 to 8191 that identifies the MPID.
cos	(Optional) Indicates the class of service (CoS) for CFM packets.
cos-value	(Optional) Integer from 0 to 7 that specifies the CoS.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE cfm mep domain command.

Examples

The following example shows how to configure the **cfm mep domain** command:

```
Device(config)#ethernet cfm domain CUSTOMER level 7
Device(config-ecfm)#service customer_100 evc evc_100
```

cos

To set the class of service (CoS) for a Cisco IOS IP Service Level Agreements (SLAs) Ethernet operation, use the **cos** command in the appropriate submode of IP SLA configuration or IP SLA Ethernet monitor configuration mode. To return to the default value, use the **no** form of this command.

cos-value	Class of service (CoS) value. The range is from 0 to 7. The default is 0.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE cos command.

Examples

The following example shows how to configure this command:

```
Interface interface-name
 cfm mep domain domain-name mpid id service service-name
  alarm notification all*
  cos 0-7
```

ethernet cfm ieee

To enable the Ethernet Connectivity Fault Management 802.1ag Standard (CFM IEEE) version of CFM, use the **ethernet cfm ieee** command in global configuration mode. To disable the CFM IEEE version, use the **no** form of this command.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE ethernet cfm ieee command.

Examples

```
Device(config)# ethernet cfm ieee
```

ethernet cfm global

To enable Ethernet connectivity fault management (CFM) globally on a device, use the **ethernet cfm global** command in global configuration mode. To disable CFM globally on a device, use the **no** form of this command.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE ethernet cfm global command.

Examples

```
Device(config)# ethernet cfm global
```

ethernet oam

To enable Ethernet operations, maintenance, and administration (OAM) on an interface, use the **ethernet oam** command in interface configuration mode. To disable Ethernet OAM on an interface, use the **no** form of this command.

mode	(Optional) Sets the OAM client mode.
passive	(Optional) Sets the OAM client mode to passive. In passive mode, a device cannot initiate discovery, inquire about variables, or set loopback mode.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE ethernet oam command.

Examples

The following example shows how to activate an Ethernet OAM interface that was previously configured to be in passive mode:

```
Device(config)# interface gigabitethernet 0/1
Device(config-if)# ethernet oam mode passive
```

ethernet oam remote-loopback

To turn on or off Ethernet operations, maintenance, and administration (OAM) remote loopback functionality on an interface, use the **ethernet oam remote-loopback**command in privileged EXEC mode. This command does not have a **no** form.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE ethernet oam remote-loopback command.

Examples

The following example shows when a remote loopback session is supported:

```
Device# ethernet oam remote-loopback supported
```

ethernet loopback permit

To configure an Ethernet data-plane loopback session on the interface, use the **ethernet loopback permit** command in interface configuration mode. To disable the Ethernet data-plane loopback session on the interface, use the **no** form of this command.

Syntax Description

external	Allows the activation of loopback of the traffic from the wire.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE ethernet loopback permit command.

Examples

The following example shows the how to configure an Ethernet data-plane loopback session:

```
Device(config)# interface ethernet 0/1
Device(config-if)# ethernet loopback permit external
```

snmp-server enable traps ethernet cfm cc

To enable Simple Network Management Protocol (SNMP) trap generation for Ethernet connectivity fault management (CFM) continuity check events, use the **snmp-server enable traps ethernet cfm cc** command in global configuration mode. To disable SNMP trap generation for Ethernet CFM continuity check events, use the **no** form of this command.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE snmp-server enable traps ethernet cfm cc command.

Examples

```
Device(config)# snmp-server enable traps ethernet cfm cc
```

snmp-server enable traps ethernet cfm crosscheck

To enable Simple Network Management Protocol (SNMP) trap generation for Ethernet connectivity fault management (CFM) continuity check events, in relation to the cross-check operation between statically configured maintenance endpoints (MEPs) and those learned via continuity check messages (CCMs), use the **snmp-server enable traps ethernet cfm crosscheck** command in global configuration mode. To disable SNMP trap generation for these continuity check events, use the **no** form of this command.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE snmp-server enable traps ethernet cfm crosscheck command.

Examples

```
Device (config)# snmp-server enable traps ethernet cfm crosscheck
```

ethernet evc

To define an Ethernet virtual connection (EVC) and to enter EVC configuration mode, use the **ethernet evc** command in global configuration mode. To delete the EVC, use the **no** form of this command.

Supported Parameters

evc-id	String from 1 to 100 characters that identifies the EVC.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

For more information about this command, see the Cisco IOS XE ethernet evc command.

Examples

```
Device(config)# ethernet evc evc-id
```

ethernet cfm domain level

To define a connectivity fault management (CFM) maintenance domain at a particular maintenance level and enter Ethernet CFM configuration mode, use the **ethernet cfm domain level** command in global configuration mode. To remove the CFM domain at the specified level, use the **no** form of this command.

Supported Parameters

domain-name	String of a maximum of 154 characters that identifies the domain.
level-id	Integer from 0 to 7 that identifies the maintenance level.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE ethernet cfm domain level command.

Examples

```
ethernet cfm domain domain-name level level-id
  id dns dns-name
  mep ccm-hold-time hours
  mep ccm-fastage enable
  mep archive-hold-time minutes
  sender-id chassis
  service vpn-id vpn-id port
  service vlan-id vlan-id port
  service number MA-number port
  service short-ma-name port
  service short-ma-name evc evc-name vlan vlanid direction down
```

offload sampling

To configure offload sampling rate, use the **offload sampling** command in the Ethernet CFM configuration mode. To return to the default value, use the **no** form of this command.

offload sampling *sample-rate*

no offload sampling

Syntax Description

sample-rate	Configure the Offload sampling rate for each CCM interval. *Range*: 10 to 10,000

Command Modes

Ethernet CFM service configuration (config-ecfm-srv)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

You configure CFM Sessions Hardware sessions for effective CPU utilization by offloading the one second CCM interval sessions on the hardware. Effective Cisco IOS XE Catalyst SD-WAN Release 17.5.1a, an Cisco IOS XE Catalyst SD-WAN device can offload the one second interval CCM sessions on hardware as well. You can enable this feature for 1 second offload sampling rate by configuring the **offload sampling 10** command on the router. This is not mandatory for all CFM sessions.

The offload sampling configuration means that when rmep session is created, the CCM packet from rmep will be punted to PI every offload sampling value. The actual punt interval time is [ccm interval * offload sampling]. For example, if CCM interval is 100ms, and the offload sampling is 100, then the punt interval of CCM packet from rmep is 100ms*100=10s. For CCM interval of 100ms/10ms/3.3ms, the default offload sampling value is 100.

ASR1000 routers can offload sessions with CCM interval of 100 milliseconds, 10 milliseconds, and 3.3 milliseconds. CCM session with 1 second interval does not get offloaded by default. To offload the CCM session with 1 second, configure the sampling rate (offload sampling). The CCM session with 10 minutes, 1 minute, and 10 seconds are not offloaded.

The suggested offload sampling for each CCM interval is as follows:

- 1s - 10
- 100ms - 100
- 10ms - 1000
- 3.3ms - 2000

To offload CCM sessions with 1 second, you must configure the hardware offload sampling rate. This example given below configures the offload sampling rate as 10 seconds.

Examples

```
Device(config)#ethernet cfm domain domain1 level 6
Device(config-ecfm)#service USER_SRV evc USER_EVC vlan 100 direction down
Device(config-ecfm-srv)#continuity-check
Device(config-ecfm-srv)#continuity-check interval 1s
Device(config-ecfm-srv)#offload sampling 10
```

sender-id

To indicate the contents of the Sender ID TLV field transmitted in Ethernet connectivity fault management (CFM) messages for members of a maintenance domain, use the **sender-id** command in Ethernet CFM configuration mode. To send no sender ID information, use the **no** form of this command.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE sender-id command.

Examples

```
Device(config)#ethernet cfm domain domain-name level 5
Device(config-ecfm)#sender-id chassis
```

service (CFM-srv)

To configure a maintenance association within a maintenance domain and enter Ethernet connectivity fault management (CFM) service configuration mode (config-ecfm-srv), use the **service** command in Ethernet CFM configuration mode. To remove the configuration, use the **no** form of this command.

Supported Parameters

ma-name	Short maintenance association name.
ma-num	Integer from 0 to 65535 that identifies the maintenance association.
vlan-id	Configures a primary VLAN.
vlan-id	Integer from 1 to 4094 that identifies the primary VLAN.
vpn-id	Configures a virtual private network (VPN).
vpn-id	Integer from 1 to 32767 that identifies the VPN.
port	(Optional) Configures a DOWN service direction without a VLAN association.
vlan	(Optional) Configures a VLAN.
direction	(Optional) Configures the service direction. The default is “up.”
down	(Optional) Configures the direction toward the LAN.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE service (CFM-srv) command.

Examples

```
ethernet cfm domain domain-name level level-id
 id dns dns-name
 mep ccm-hold-time hours
 mep ccm-fastage enable
 mep archive-hold-time minutes
 sender-id chassis
 service vpn-id vpn-id port
 service vlan-id vlan-id port
 service number MA-number port
 service short-ma-name port
 service short-ma-name evc evc-name vlan vlanid direction down
```

service evc

To set a universally unique ID for a customer service instance (CSI) within a maintenance domain, use the **service evc** command in Ethernet CFM configuration mode. To remove a universally unique ID for a service within a maintenance domain, use the **no** form of this command.

Supported Parameters

service	Specifies the service instance.
evc	Specifies the Ethernet virtual circuit (EVC).
evc-name	String that identifies the Ethernet virtual circuit (EVC).
vlan	Specifies the VLAN.
vlan-id	String the VLAN ID. Range is from 1 to 4094.
direction	Specifies the service direction.
down	Specifies the direction towards the LAN.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE service evc command.

Examples

```
ethernet cfm domain domain-name level level-id
 id dns dns-name
 mep ccm-hold-time hours
 mep ccm-fastage enable
 mep archive-hold-time minutes
 sender-id chassis
 service vpn-id vpn-id port
 service vlan-id vlan-id port
 service number MA-number port
 service short-ma-name port
 service short-ma-name evc evc-name vlan vlanid direction down
```

continuity-check

To enable the transmission of continuity check messages (CCMs), use the **continuity-check** command in Ethernet connectivity fault management (CFM) service configuration mode. To disable message transmission, use the **no** form of this command.

Supported Parameters

interval	(Optional) Configures the time period between message transmissions.
loss-threshold	(Optional) Sets the number of CCMs that should be missed before declaring that a remote maintenance endpoint (MEP) is down.
threshold	(Optional) Integer from 2 to 255. The default is 3.

Command History

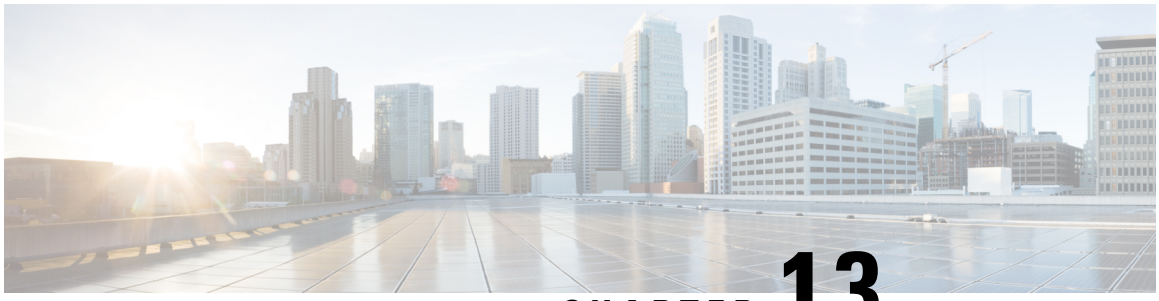
Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE continuity-check command.

Examples

```
ethernet cfm domain domain-name level level-id
 id dns dns-name
 mep ccm-hold-time hours
 mep ccm-fastage enable
 mep archive-hold-time minutes
 sender-id chassis
 service vpn-id vpn-id port
 service vlan-id vlan-id port
 service number MA-number port
 service short-ma-name port
 service short-ma-name evc evc-name vlan vlanid direction down
  continuity-check
  continuity-check [interval cc-interval]
  continuity-check loss-threshold threshold
  ais period 1 or 60
  ais level 0-7
  ais expiry-threshold 0-255
  ais suppress-alarms
  maximum meps 1-65535
  sender-id chassis
  offload sampling sample
```



CHAPTER 13

Cisco Survivable Remote Site Telephony Commands

- Cisco Survivable Remote Site Telephony Commands, on page 147
- SRST Commands, on page 147

Cisco Survivable Remote Site Telephony Commands

Table 11: Feature History

Feature Name	Release Information	Description
Cisco Survivable Remote Site Telephony Commands	Cisco IOS XE Catalyst SD-WAN Release 17.14.1a Cisco Catalyst SD-WAN Manager Release 20.14.1	This feature enables you to configure Cisco Survivable Remote Site Telephony (SRST) commands on Cisco IOS XE Catalyst SD-WAN devices using Cisco SD-WAN Manager device CLI templates or CLI add-on feature templates.

This documentation describes the commands for configuring Cisco Survivable Remote Site Telephony (SRST) commands that are tested and verified on a Cisco IOS XE Catalyst SD-WAN device using a Cisco SD-WAN Manager CLI template or a CLI add-on feature template.

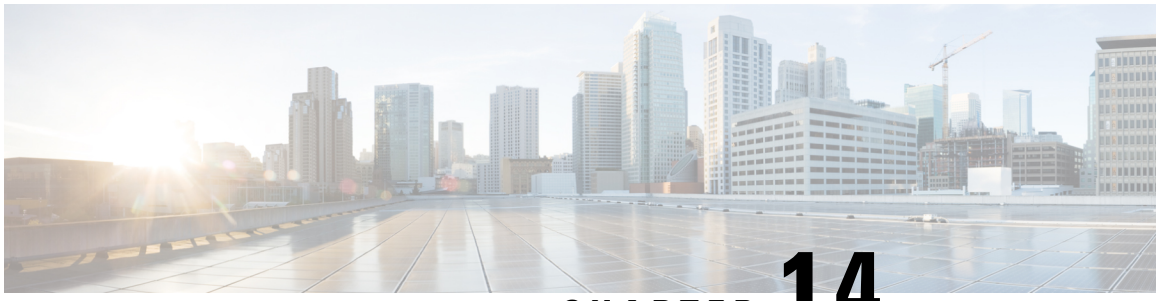
These commands are supported beginning with Cisco IOS XE Catalyst SD-WAN Release 17.14.1a and Cisco Catalyst SD-WAN Manager Release 20.14.1.

SRST Commands

The following table lists the commands that are supported by Cisco Catalyst SD-WAN CLI templates for SRST. Click a command name in the **Command** column to view information about the command, its syntax, and its use.

Table 12: Cisco Catalyst SD-WAN CLI Template Commands for SRST

Command	Description
http client secure-ciphersuite	Sets the secure encryption cipher suite for the HTTP client.
transport-tcp-tls (call-manager-fallback)	Configures a specific TLS version for Unified Secure SCCP SRST, in call-manager-fallback mode.



CHAPTER 14

Cisco TrustSec

- aaa authorization network, on page 150
- aaa group server radius, on page 150
- aaa server radius dynamic-author, on page 151
- accept-lifetime, on page 151
- client, on page 152
- cryptographic-algorithm, on page 152
- cts authorization list network, on page 153
- cts credentials, on page 154
- cts role-based enforcement, on page 154
- cts role-based permissions, on page 155
- cts role-based sgt-map , on page 156
- cts sgt, on page 156
- cts sxp connection peer, on page 157
- cts sxp default key-chain, on page 158
- cts sxp default password, on page 159
- cts sxp default source-ip, on page 160
- cts sxp enable, on page 160
- cts sxp listener hold-time, on page 161
- cts sxp log binding-changes, on page 161
- cts manual, on page 162
- cts sxp node-id, on page 162
- cts sxp reconciliation period, on page 163
- cts sxp retry period, on page 163
- cts sxp speaker hold-time, on page 164
- domain stripping, on page 164
- ip radius source-interface, on page 165
- ip vrf forwarding, on page 165
- key, on page 165
- key chain, on page 166
- key-string, on page 166
- port, on page 167
- recv-id, on page 167
- send-id, on page 168

• send-lifetime, on page 169
• server-private (RADIUS), on page 169

aaa authorization network

To set authorization for all network-related service requests, use the **aaa authorization network** command in global configuration mode.

aaa authorization network *authorization-list-name* [**group**] *group_name*

Syntax Description

authorization-list-name	Character string used to name the list of authorization methods activated when a user logs in.
group	Uses a subset of RADIUS servers for authentication as defined by the server group **group-name**
group_name	Server group name.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Examples

The following example shows how to set an authorization method list to the RADIUS server group in local web authentication

```
Device# config-transaction
Device(config)# aaa authorization network webauth_radius group ISE_group
Device(config)#
```

aaa group server radius

To group different RADIUS server hosts into distinct lists and distinct methods, enter the **aaa group server radius** command in global configuration mode. To remove a group server from the configuration list, enter the **no** form of this command.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

For more information about this command, see the Cisco IOS XE aaa group server radius

Examples

The following example shows the configuration of an AAA group server named radgroup1 that comprises three member servers:

```
Device# config-transaction
Device(config)# aaa group server radius radgroup1
Device(config-sg-radius)#server-private 10.251.1.1 timeout 5 retransmit 3 pac key 6
JTfGZMb[edH[G_V[MfQYKN^N]QeeBbLeB
Device(config-sg-radius)#ip radius source-interface GigabitEthernet0/0/1.100
Device(config-sg-radius)#ip vrf forwarding 1
Device(config-sg-radius)#
```

Note If auth-port and acct-port are not specified, the default value of auth-port is 1812 and the default value of acct-port is 1813.

aaa server radius dynamic-author

To configure a device as an authentication, authorization, and accounting (AAA) server to facilitate interaction with an external policy server, use the **aaa server radius dynamic-author**command in global configuration mode. To remove this configuration, use the **no** form of this command.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

For more information about this command, see the Cisco IOS XE aaa server radius dynamic-author

Examples

The following example configures the ISG to act as a AAA server when interacting with the client at IP address 10.12.12.12:

```
Device# config-transaction
Device#(config)# aaa server radius dynamic-author
Device#(config-locsvr-da-radius)# client 10.12.12.12 vrf 1 server-key 6
PhHSFDUiS_abVCScDPYgYPJgXYXP[A^DY
Device#(config-locsvr-da-radius)#
```

accept-lifetime

To set the time period during which the authentication key on a key chain is received as valid, use the **accept-lifetime**command inkey chain key configuration mode. To revert to the default value, use the **no** form of this command.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

For more information about this command, see the Cisco IOS XE accept-lifetime

Examples

The following show how to specify the time entered in Cisco vManage for which the key is valid to be accepted for TCP-AO authentication.

Specify the start-time in the local time zone. By default, the start-time corresponds to UTC time. The end-time can be specified in 3 ways - infinite (no expiry), duration (1- 2147483646 sec), exact time – either UTC or local.

```
Device# config-transaction
Device(config)#key chain key6 tcp
Device(config-keychain)# key 2000
Device(config-keychain-key)# accept-lifetime local 18:00:00 Jan 12 2021 06:00:00 Jan 12
2022
Device(config-keychain-key)#
```

client

To specify a RADIUS client from which a device will accept Change of Authorization (CoA) and disconnect requests, use the **client** command in dynamic authorization local server configuration mode. To remove this specification, use the **no** form of this command.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

For more information about this command, see the Cisco IOS XE client

Examples

The following example configures the router to accept requests from the RADIUS client at IP address 10.0.0.1:

```
Device# config-transaction
Device#(config)# aaa server radius dynamic-author
Device#(config-locsvr-da-radius)# client 10.0.0.1 vrf 1 server-key 6
gWTLbecJKOQcFcIbJNR[]WKP_g^TRacRF
Device#(config)#
```

cryptographic-algorithm

To specify the TCP cryptographic algorithm for a TCP-AO key, use the **cryptographic-algorithm** command in key chain key configuration mode. To disable this feature, use the **no** form of this command.

cryptographic-algorithm *algorithm*

no cryptographic-algorithm *algorithm*

Syntax Description

algorithm	Specify one of the following authentication algorithms: • `aes-128-cmac`- AES-128-CMAC algorithm • `hmac-sha-1`- HMAC-SHA-1 algorithm • `hmac-sha-256`- HMAC-SHA-256 algorithm

Command Default

No algorithm is specified.

Command Modes

Key chain key configuration (config-keychain-key)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

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.

The following example configures a simple key chain for a TCP-AO enabled connection.

```
Device#config-transaction
Device(config)# key chain kc1 tcp
Device(config-keychain)# key 7890
Device(config-keychain-key)# send-id 215
Device(config-keychain-key)# recv-id 215
Device(config-keychain-key)# key-string klomn
Device(config-keychain-key)# cryptographic-algorithm hmac-sha-1
Device(config-keychain-key)#
```

cts authorization list network

To specify a list of AAA servers for the Cisco TrustSec (CTS) seed device to use, use the **cts authorization list network** command in global configuration mode. To stop using the list during authentication, use the **no** form of this command.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

For more information about this command, see the Cisco IOS XE cts authorization list network

Examples

The following example shows how to specify a list of AAA servers for a CTS seed device:

```
Device# config-transaction
Device(config)# aaa group server radius radgroup1
Device(config-sg-radius)#server-private 10.251.1.1 timeout 5 retransmit 3 pac key 6
JTfGZMb[edH[G_V[MfQYKN^N]QeeBbLeB
Device(config-sg-radius)#ip radius source-interface GigabitEthernet0/0/1.100
```

```
Device(config-sg-radius)#ip vrf forwarding 1
Device(config-sg-radius)#
```

```
Device# config-transaction
Device(config)# aaa authentication enable default enable
Device(config)# aaa authentication login default local group radius-1
Device(config)# aaa authorization console
Device(config)# aaa authorization exec default local group radius-1
Device(config)# aaa authorization network cts-mlist group radius-1
Device(config)#
```

```
Device# config-transaction
Device(config)# cts authorization list cts-mlist
Device(config)#
```

cts credentials

To specify the Cisco TrustSec (CTS) ID and password of the network device, use the **cts credentials** command in privileged EXEC mode. To delete the CTS credentials, use the **clear cts credentials** command.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

For more information about this command, see the Cisco IOS XE cts credentials

Examples

The following example configures himalaya and cisco as the CTS device ID and password:

```
Device# cts credentials id himalaya password cisco

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

The following example changes the CTS device ID and password to atlas and cisco123:

```
Device# cts credentials id atlas password cisco123

A different device ID is being configured.
This may disrupt connectivity on your CTS links.
Are you sure you want to change the Device ID? [confirm] y
TS device ID and password have been inserted in the local keystore. Please make sure that
the same ID and password are configured in the server database.
```

The following example displays the CTS device ID and password state:

```
Device# show cts credentials

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

cts role-based enforcement

To enable role-based access control globally and on specific Layer 3 interfaces using Cisco TrustSec, use the **cts role-based enforcement** command in global configuration mode and interface configuration mode

respectively. To disable the enforcement of role-based access control at an interface level, use the **no** form of this command.

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

For more information about this command, see the Cisco IOS XE cts role-based enforcement

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

```
Device# config-transaction
Device(config)# interface gigabitethernet 1/1/3
Device(config-if)# cts role-based enforcement
Device(config-if)#
```

cts role-based permissions

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

cts role-based permissions { { [**default** | **from** | [*source-sgt*] | **to** | [*dest-sgt*]] } }

no cts role-based permissions { { [**default** | **from** | [*source-sgt*] | **to** | [*dest-sgt*]] } }

Syntax Description

default	Specifies the default permissions list. Every cell (an SGT pair) for which, security group access control list (SGACL) permission is not configured statically or dynamically falls under the default category. .
from	Specifies the source group tag of the filtered traffic.
source-sgt	Security Group Tag (SGT). Valid values are from 0 to 65519.
dest-sgt	Security Group Tag (SGT). Valid values are from 2 to 65519.

Command Default

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

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

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** 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.

Examples

The following example shows how to enter CTS manual interface configuration mode on an interface:

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

cts role-based sgt-map

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

Supported Parameters

interface-type	Specifies the type of interface. For example, ethernet. The specified SGT is mapped to traffic from this logical or physical Layer 3 interface.
sgtsgt-number	Specifies the SGT number from 0-65535.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

For more information about this command, see the Cisco IOS XE cts role-based sgt-map

Examples

The following example shows how to manually map a source IP address to an SGT on a Cisco ASR 1000 series router:

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

cts sgt

To manually assign a Security Group Tag (SGT) number to a network device, use the **cts sgt** command in global configuration mode. Use the **no** form of the command to remove the tag.

cts sgt *tag-number*
no cts sgt *tag-number*

Supported Parameters

tag-number	Configures the SGT for packets sent from this device. The *tag-number* argument is in decimal format. The range is from 1 to 65533.

Command Default

No SGT number is assigned

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines In Cisco TrustSec, the authentication server assigns an SGT to the device for packets originating from the device. You can manually configure an SGT to be used if the authentication server is not accessible, but an authentication server-assigned SGT will take precedence over a manually assigned SGT.

Examples The following example shows how to enter CTS manual interface configuration mode on an interface:

```
Device# config-transaction
Device(config)# cts sgt 1234
Device(config)#
```

cts sxp connection peer

Use the **cts sxp connection peer** command in global configuration mode to specify

- the Cisco TrustSec Security Group Tag (SGT) Exchange Protocol (CTS-SXP) peer IP address
- if a password is used for the peer connection or a TCP key-chain should be used to provide TCP-AO authentication
- the global hold-time period for a listener or speaker device
- if the connection is bidirectional.

To remove these configurations for a peer connection, use the **no** form of this command.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines For more information about this command, see the Cisco IOS XE cts sxp connection peer

Examples The following example shows how to enable CTS-SXP and configure the CTS-SXP peer connection on Device_A, a speaker, for connection to Device_B, a listener with the password option for TCP MD5 authentication: :

```
Device_A> enable
Device_A# config-transaction
Device_A#(config)# cts sxp enable
Device_A#(config)#cts sxp node-id ipv4 10.30.1.1
Device_A#(config)# cts sxp default password Cisco123
Device_A#(config)# cts sxp default source-ip 10.10.1.1
Device_A#(config)# cts sxp connection peer 10.20.2.2 password default mode local speaker
hold-time 0 vrf 7
Device_A#(config)#
```

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

```
Device_B> enable
Device_B# config-transaction
Device_B(config)# cts sxp enable
Device_B#(config)#cts sxp node-id ipv4 10.30.1.2
Device_B(config)# cts sxp default password Cisco123
Device_B(config)# cts sxp default source-ip 10.20.2.2
Device_B(config)# cts sxp connection peer 10.10.1.1 password default mode local listener
hold-time 0 vrf 7
Device_B#(config)#
```

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

The following example shows how to configure the CTS-SXP peer connection on Device_A, a speaker, for connection to Device_B, a listener without a password or key chain option:

```
Device_A(config)# cts sxp connection peer 10.51.51.1 source 10.51.51.2 password none mode
local speaker hold-time 0 vrf 7
Device_A(config)#
```

```
Device_B(config)# cts sxp connection peer 10.51.51.2 source 10.51.51.1 password none mode
local listener hold-time 0 vrf 7
Device_B(config)#
```

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

```
Device_A> enable
Device_A# config-transaction
Device_A#(config)# cts sxp enable
Device_A#(config)# cts sxp default password Cisco123
Device_A#(config)# cts sxp node-id ipv4 10.30.1.1
Device_A#(config)# cts sxp default source-ip 10.10.1.1
Device_A#(config)# cts sxp connection peer 10.20.2.2 password default mode local both
Device_A#(config)#cts sxp connection peer 10.20.2.2 password default mode local both vrf 7
Device_A#(config)#
```

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

```
Device_A> enable
Device_A# config-transaction
Device_A#(config)# cts sxp enable
Device_A#(config)# cts sxp node-id ipv4 10.30.1.2
Device_A#(config)# cts sxp default key-chain sxp_1
Device_A#(config)# cts sxp connection peer 10.2.2.2 password key-chain mode local speaker
hold-time 0 vrf 7
Device_A#(config)#
```

cts sxp default key-chain

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

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

For more information about this command, see the Cisco IOS XE cts sxp default key-chain

Example

In the following example, a TCP-AO key chain named sxp_1 is configured as the default key chain for CTS SXP sessions using TCP-AO.

```
Device> enable
Device# config-transaction
Device(config)# cts sxp default key-chain key6
Device(config)# cts sxp connection peer 10.30.1.1 source 10.201.1.2 password key-chain mode
 local speaker hold-time 0 vrf 1
Device(config)# cts sxp enable
Device(config)# cts sxp node-id ipv4 10.30.1.1
Device(config)#
```

cts sxp default password

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

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

For more information about this command, see the Cisco IOS XE cts sxp default password

Examples

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

```
Device_A# config-transaction
Device_A#(config)# cts sxp enable
Device_A#(config)# cts sxp default password Cisco123
Device_A#(config)# cts sxp default source-ip 10.10.1.1
Device_A#(config)# cts sxp node-id ipv4 10.30.1.1
Device_A#(config)# cts sxp connection peer 10.20.2.2 password default mode local speaker
Device_A#(config)#
```

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

```
Device_B# config-transaction
Device_B(config)# cts sxp enable
Device_B(config)# cts sxp default password Cisco123
Device_B(config)# cts sxp default source-ip 10.20.2.2
Device_B#(config)#cts sxp node-id ipv4 10.30.1.2
Device_B(config)# cts sxp connection peer 10.10.1.1 password default mode local listener
Device_B#(config)#
```

cts sxp default source-ip

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

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

For more information about this command, see the Cisco IOS XE cts sxp default source-ip

Examples

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

```
Device_A# config-transaction
Device_A#(config)# cts sxp enable
Device_A#(config)# cts sxp default password Cisco123
Device_A#(config)# cts sxp default source-ip 10.10.1.1
Device_A#(config)# cts sxp node-id ipv4 10.30.1.1
Device_A#(config)# cts sxp connection peer 10.20.2.2 password default mode local speaker
Device_A#(config)#
```

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

```
Device_B# config-transaction
Device_B(config)# cts sxp enable
Device_B(config)# cts sxp default password Cisco123
Device_B(config)# cts sxp default source-ip 10.20.2.2
Device_B#(config)# cts sxp node-id ipv4 10.30.1.2
Device_B(config)# cts sxp connection peer 10.10.1.1 password default mode local listener
Device_B#(config)#
```

cts sxp enable

To enable the Cisco TrustSec Security Group Tag (SGT) Exchange Protocol (CTS-SXP) on a device, use the **cts sxp enable** command in global configuration mode. To disable the CTS-SXP on a device, use the **no** form of this command

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

For more information about this command, see the Cisco IOS XE cts sxp enable

Examples

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

```
Device_A# config-transaction
Device_A#(config)# cts sxp enable
Device_A#(config)# cts sxp node-id ipv4 10.30.1.1
Device_A#(config)# cts sxp default password Cisco123
Device_A#(config)# cts sxp default source-ip 10.10.1.1
Device_A#(config)# cts sxp connection peer 10.20.2.2 password default mode local speaker
Device_A#(config)#
The following example shows how to configure the CTS-SXP peer connection on Device_B, a
listener, for connection to Device_A, a speaker:
Device_B# config-transaction
Device_B(config)# cts sxp enable
Device_B(config)# cts sxp default password Cisco123
Device_B#(config)# cts sxp node-id ipv4 10.30.1.2
Device_B(config)# cts sxp default source-ip 10.20.2.2
Device_B(config)# cts sxp connection peer 10.10.1.1 password default mode local listener
Device_B(config)#
```

cts sxp listener hold-time

To configure the global hold-time period of a listener network device in a Cisco TrustSec Security Group Tag (SGT) Exchange Protocol version 4 (SXPv4) network, use the **cts sxp listener hold-time** command in global configuration mode. To remove the hold time from the listener device, use the **no** form of this command.

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

For more information about this command, see the Cisco IOS XE cts sxp listener hold-time

The following example shows how to configure the hold time period of a listener device for a minimum of 300 seconds and a maximum of 500 seconds:

```
Device> enable
Device# config-transaction
Device(config)# cts sxp listener hold-time 300 500
Device(config)#
```

cts sxp log binding-changes

To enable logging for IP-to-Cisco TrustSec Security Group Tag (SGT) Exchange Protocol (CTS-SXP) binding changes, use the **cts sxp log binding-changes** command in global configuration mode. To disable logging, use the **no** form of this command.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

For more information about this command, see the Cisco IOS XE cts sxp log binding-changes

Examples

The following example shows how to enable logging for IP-to-Cisco TrustSec Security Group Tag (SGT) Exchange Protocol (CTS-SXP) binding changes:

```
Device# config-transaction
Device#(config)# cts sxp log binding-changes
Device#(config)#
```

cts manual

To manually enable an interface for Cisco TrustSec Security (CTS), use the **cts manual** command in interface configuration mode.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

For more information about this command, see the Cisco IOS XE cts manual

Examples

The following example shows how to enter CTS manual interface configuration mode on an interface:

```
Device# config-transaction
Device(config)# interface gigabitethernet 0
Device(config-if)# cts manual
Device(config-if-cts-manual))#
```

The following example shows how to remove the CTS manual configuration from an interface:

```
Device# config-transaction
Device(config)# interface gigabitethernet 0
Device(config-if)# no cts manual
Device(config-if)#
```

cts sxp node-id

To configure the node ID of a network device for Cisco TrustSec (CTS) Security Group Tag (SGT) Exchange Protocol version 4 (SXPv4), use the **cts sxp node-id** command in global configuration mode. To remove the node ID, use the **no** form of this command.

When you need to change a Node ID, you must first disable SXP and then push the template to the device. Then, you change the Node ID, and then push the template to the device again.

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

For more information about this command, see the Cisco IOS XE cts sxp node-id

The following example shows how to configure the node ID of a network device for Cisco TrustSec (CTS) Security Group Tag (SGT) Exchange Protocol version 4 (SXPv4).

```
Device# config-transaction
Device(config)# cts sxp node-id ipv4 10.16.1.3
Device(config)#
```

cts sxp reconciliation period

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

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

For more information about this command, see the Cisco IOS XE cts sxp reconciliation period

Examples

The following example shows how to change the Cisco TrustSec Security Group Tag (SGT) Exchange Protocol (CTS-SXP) reconciliation period:

```
Device# config-transaction
Device#(config)# cts sxp reconciliation period 120
Device(config)#
```

cts sxp retry period

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

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

For more information about this command, see the Cisco IOS XE cts sxp retry period

Examples

The following example shows how to change the Cisco TrustSec Security Group Tag (SGT) Exchange Protocol (CTS-SXP) retry period timer:

```
Device# config-transaction
Device#(config)# cts sxp retry period 60
Device(config)#
```

cts sxp speaker hold-time

To configure the global hold-time period of a speaker network device in a Cisco TrustSec Security Group Tag (SGT) Exchange Protocol version 4 (SXPv4) network, use the **cts sxp speaker hold-time** command in global configuration mode. To remove the hold time from the speaker device, use the **no** form of this command.

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

For more information about this command, see the Cisco IOS XE cts sxp speaker hold-time

The following example shows how to configure the minimum hold time period of a speaker device for 300 seconds:

```
config-transaction
Device(config)# cts sxp speaker hold-time 300
Device(config)#
```

domain stripping

To configure domain stripping at the server group level, use the **domain-stripping** command in server group RADIUS configuration mode. To disable the configuration, use the **no** form of this command.

Supported Parameters

right-to-left	(Optional) Terminates the string at the first delimiter going from right to left.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

For more information about this command, see the Cisco IOS XE domain stripping

Examples

The following example shows how to configure domain stripping at the server group level:

```
Device# configure transaction
Device(config)# aaa server radius dynamic-author
Device(config-locsvr-da-radius)# client 77.251.1.1 vrf 1 server-key 0
$CRYPT_CLUSTER$8p6dnAgrJ00J5nT2ibIz+A==$7hds/zxmCbjtkbAJlKynPQ==
Device(config-locsvr-da-radius)# domain stripping right-to-left
Device(config-locsvr-da-radius)#
```

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.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

For more information about this command, see the Cisco IOS XE ip radius source-interface

Examples

The following example shows how to configure RADIUS to use the IP address of subinterface s2 for all outgoing RADIUS packets:

```
Device# config-transaction
Device(config)# aaa group server radius radgroup1
Device#(config-sg-radius)# ip radius source-interface GigabitEthernet0/0/1.100
Device#(config-sg-radius)#
```

ip vrf forwarding

To associate a Virtual Private Network (VPN) routing and forwarding (VRF) instance with a Diameter peer, use the **ip vrf forwarding** command in Diameter peer configuration mode. To enable Diameter peers to use the global (default) routing table, use the no form of this command.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

For more information about this command, see the Cisco IOS XE ip vrf forwarding

Examples

The following example shows how to configure a VRF:

```
config-transaction
Device(config)# aaa group server radius radius-1
Device# (config-sg-radius)# ip vrf forwarding 1
Device(config-sg-radius)#
```

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.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

For more information about this command, see the Cisco IOS XE key

Examples

You configure TCP Authentication Option (TCP-AO) for SXP where you configure keys on both the peers communicating through a TCP connection.

This example shows how to create a key with the specified key-id.

```
Device# config-transaction
Device(config)#key chain key6 tcp
Device(config-keychain)# key 2000
Device(config-keychain-key)#
```

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.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

For more information about this command, see the Cisco IOS XE key chain

Examples

You configure TCP Authentication Option (TCP-AO) for SXP where you configure the key chain on both the peers communicating through a TCP connection.

This example shows how to create a TCP-AO key chain with the specified name.

```
Device# config-transaction
Device(config)#key chain key6 tcp
Device(config-keychain)#
```

key-string

To specify the authentication string for a key, use the **key-string**command in key chain key configuration mode. To remove the authentication string, use the **no** form of this command.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

For more information about this command, see the Cisco IOS XE key-string

Examples

This example show how to specify the master-key for deriving traffic keys.

The master-keys must be identical on both peers. If the master-keys do not match, authentication fails and segments may be rejected by the receiver.

```
Device# config-transaction
Device(config)#key chain key6 tcp
Device(config-keychain)# key 2000
Device(config-keychain-key)# key-string 6 _RPB[dVI]SO^BAOVNMKATgOZKMXFGXFTa
```

port

To specify the port on which a device listens for RADIUS requests from configured RADIUS clients, use the **port** command in dynamic authorization local server configuration mode. To restore the default, use the **no** form of this command.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

For more information about this command, see the Cisco IOS XE port

Examples

The following example specifies port 1650 as the port on which the device listens for RADIUS requests:

```
Device# config-transaction
Device#(config)# aaa server radius dynamic-author
Device#(config-locsvr-da-radius)# client 10.0.0.1
Device#(config-locsvr-da-radius)# port 1650
Device#(config-locsvr-da-radius)#
```

recv-id

To specify the receive ID for a TCP-AO key chain, use the **recv-id** command in the key chain key configuration mode. To remove the receive ID, use the **no** form of this command.

recv-id *ID*

no recv-id *ID*

Supported Parameters

ID	Specifies the receive identifier. An integer between 0 to 255.

Command Modes

Key chain key configuration (config-keychain-key)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

The **send-id** on the device must match the **recv-id** on the other device and vice versa.

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.

The following example configures a simple key chain for a TCP-AO enabled connection.

```
Device# config-transaction
Device(config)# key chain kc1 tcp
Device(config-keychain)# key 7890
Device(config-keychain-key)# send-id 215
Device(config-keychain-key)# recv-id 215
Device(config-keychain-key)# key-string klomn
Device(config-keychain-key)# cryptographic-algorithm hmac-sha-1
Device(config-keychain-key)# include-tcp-options
Device(config-keychain-key)#
```

send-id

To specify the send ID for a TCP-AO key chain, use the **send-id** command in the key chain key configuration mode. To remove the send ID, use the **no** form of this command.

send-id *ID*

no send-id *ID*

Supported Parameters

ID	Specifies the send identifier. An integer between 0 to 255.

Command Modes

Key chain key configuration (config-keychain-key)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

The **send-id** on the device must match the **recv-id** on the other device and vice versa.

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.

The following example configures a simple key chain for a TCP-AO enabled connection.

```
Device# config-transaction
Device(config)# key chain kc1 tcp
Device(config-keychain)# key 7890
Device(config-keychain-key)# send-id 215
Device(config-keychain-key)# recv-id 215
Device(config-keychain-key)# key-string klomn
Device(config-keychain-key)# cryptographic-algorithm hmac-sha-1
Device(config-keychain-key)# include-tcp-options
Device(config-keychain-key)#
```

send-lifetime

To set the time period during which an authentication key on a key chain is valid to be sent, use the **send-lifetime** command in key chain key configuration mode. To revert to the default value, use the **no** form of this command.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

For more information about this command, see the Cisco IOS XE send-lifetime

Examples

The following show how to specify the time entered in Cisco SD-WAN Manager for which the key is valid to be used for TCP-AO authentication.

Specify the start-time in the local time zone. By default, the start-time corresponds to UTC time. The end-time can be specified in 3 ways - infinite (no expiry), duration (1- 2147483646 sec), exact time – either UTC or local.

```
Device# config-transaction
Device(config)#key chain key6 tcp
Device(config-keychain)# key 2000
Device(config-keychain-key)# send-lifetime local 18:00:00 Jan 12 2021 01:00:00 Jan 12 2022
Device(config-keychain-key)#
```

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.

Supported Parameters

ip-address	IP address of the private RADIUS server host.
auth-port *port-number*	(Optional) User Datagram Protocol (UDP) destination port for authentication requests. The default value is 1645.
acct-port *port-number*	Optional) UDP destination port for accounting requests. The default value is 1646.

timeout *seconds*	(Optional) Time interval (in seconds) that the router waits for the RADIUS server to reply before retransmitting. This setting overrides the global value of the **radius-server timeout** command. If no timeout value is specified, the global value is used.
retransmit *retries*	(Optional) Number of times a RADIUS request is resent to a server, if that server is not responding or responding slowly. This setting overrides the global setting of the **radius-server retransmit** command.
key *string*	(Optional) Authentication and encryption key used between the router and the RADIUS daemon running on the RADIUS server. This key overrides the global setting of the **radius-server key** command. If no key string is specified, the global value is used. The *string* can be **0** (specifies that an unencrypted key follows), **6** (specifies that an advanced encryption scheme [AES] encrypted key follows), **7** (specifies that a hidden key follows), or a line specifying the unencrypted (clear-text) server key.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

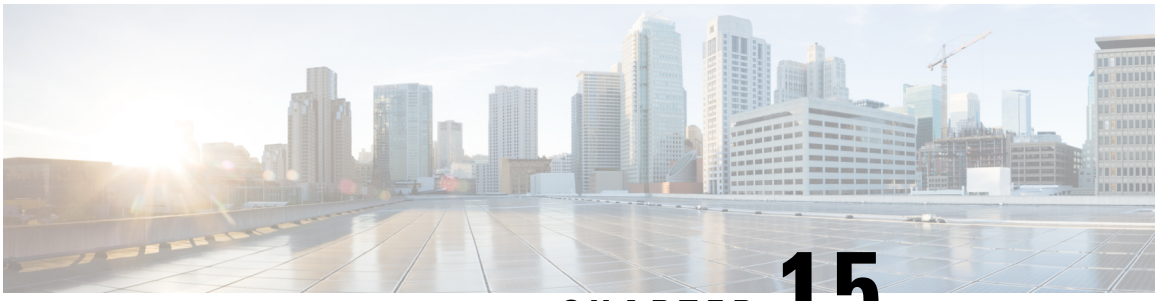
Usage Guidelines

For more information about this command, see the Cisco IOS XE server-private (RADIUS)

Examples

The following example shows how to define the sg_water RADIUS group server and associate private servers with it:

```
Device> enable
Device# config-transaction
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)#
```



CHAPTER 15

Cisco Unified Border Element Commands

Table 13: Feature History

Feature Name	Release Information	Description
Cisco Unified Border Element Configuration	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco vManage Release 20.7.1	This feature lets you configure Cisco Unified Border Element (CUBE) functionality by using Cisco IOS XE Catalyst SD-WAN device CLI templates or CLI add-on feature templates.
Secure SRST Support on Cisco Catalyst SD-WAN	Cisco IOS XE Catalyst SD-WAN Release 17.10.1a Cisco vManage Release 20.10.1	This feature enables you to configure Cisco Survivable Remote Site Telephony (SRST) commands on Cisco IOS XE Catalyst SD-WAN devices using Cisco SD-WAN Manager device CLI templates or CLI add-on feature templates. The feature also provides additional Cisco Unified Border Element (CUBE) commands that are qualified for use in Cisco Cisco SD-WAN Manager device CLI templates or CLI add-on feature templates.
Cisco Unified Border Element Configuration	Cisco IOS XE Catalyst SD-WAN Release 17.14.1a Cisco Catalyst SD-WAN Manager Release 20.14.1	This feature provides support for the following commands: • **cipher (voice class)** • **nat media-keepalive** • **secure-ciphersuite** • **transport tcp tls (sip-ua)** • **voice-class sip nat media-keepalive**

Feature Name	Release Information	Description
Secure Communications Interoperability Protocol Support in CUBE	Cisco IOS XE Catalyst SD-WAN Release 17.16.1a Cisco Catalyst SD-WAN Manager Release 20.16.1	The following commands were modified to support SCIP codec: • **voice class codec** • **video codec** *codec-type* • **codec preference** *value codec-type* • **dial peer** • **rtp payload-type codec-audio-scip** *payload-type-number* • **rtp payload-type codec-video-scip** *payload-type-number* **Note** This feature is available in its Beta version for this release, offering limited functionality.
Advanced TLS security compliance and control	Cisco IOS XE Catalyst SD-WAN Release 26.1.x Cisco Catalyst SD-WAN Manager Release 26.1.x	The commands below were modified to support insecure TLS versions in "system mode insecure" configuration mode: • cipher (voice class) • http client secure-ciphersuite • transport tcp tls

This documentation describes the commands for configuring Cisco Unified Border Element (CUBE) that are tested and verified on a Cisco IOS XE Catalyst SD-WAN device using a Cisco IOS XE Catalyst SD-WAN device CLI template or a CLI add-on feature template.

These commands are supported beginning with Cisco IOS XE Catalyst SD-WAN Release 17.7.1a and Cisco vManage Release 20.7.1.

For related information, see Cube Configuration.

• CUBE Commands, on page 172

CUBE Commands

The following table lists the commands that are supported by Cisco Catalyst SD-WAN CLI templates for CUBE configuration. Click a command name in the **Command** column to view information about the command, its syntax, and its use.

Table 14: Cisco Catalyst SD-WAN CLI Template Commands for CUBE Configuration

Command	Description
address-hiding	Hides signaling and media peer addresses from endpoints other than the gateway.
anat	Enables Alternative Network Address Types (ANAT) on a SIP trunk.
answer-address	Specifies the full E.164 telephone number to be used to identify the dial peer of an incoming call.
application (global)	Enters application configuration mode to configure applications.
asserted-id	Enables support for the asserted ID header in incoming SIP requests or response messages, and to send the asserted ID privacy information in outgoing SIP requests or response messages.
asymmetric payload	Configures SIP asymmetric payload support.
audio forced	Allows only audio and image (for T.38 Fax) media types, and drops all other media types).
authentication	Enables SIP digest authentication.
bind	Binds the source address for signaling and media packets to the IPv4 or IPv6 address of a specific interface.
block	Configures global settings to drop (not pass) specific incoming SIP provisional response messages on a CUBE.
call spike	Configures the limit on the number of incoming calls received in a short period (a call spike).
call threshold global	Enables the global resources of a gateway.
call treatment action	Configures the action that the router takes when local resources are unavailable.
call treatment cause-code	Specifies the reason for the disconnection to the caller when local resources are unavailable.
call treatment isdn-reject	Specifies the rejection cause code for ISDN calls when all ISDN trunks are busied out, but the switch ignores the busyout trunks and still sends ISDN calls into the gateway.
call treatment on	Enables call treatment to process calls when local resources are unavailable.
callmonitor	Enables the call monitoring messaging functionality on a SIP endpoint in a VoIP network.
call-route	Enables header-based routing at the global configuration level.

Command	Description
cipher (voice class)	Configures the cipher setting, and associates it to a TLS profile.
clid	Passes the network-provided ISDN numbers in an ISDN calling party information element screening indicator field, and removes the calling party name and number from the calling-line identifier in voice service voip configuration mode. Alternatively, allows the presentation of the calling number by substituting for the missing **Display Name** field in the Remote-Party-ID and From headers.
codec preference	Specifies a list of preferred codecs to use on a dial peer.
codec profile	Defines audio and video capabilities that are needed for video endpoints.
codec transparent	Enables codec capabilities to be passed transparently between endpoints in a CUBE.
conn-reuse	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Reuses the TCP connection of a SIP registration for an endpoint behind a firewall.
connection-reuse	Uses global listener port for sending requests over UDP.
contact-passing	Configures pass-through of the contact header from one leg to the other leg for 302 pass-through.
cpa	Enables the call progress analysis (CPA) algorithm for outbound VoIP calls and to set CPA parameters.
credentials	Configures a SIP TDM gateway or CUBE to send a SIP registration message when in the UP state.
crypto signaling	Identifies the **trustpoint** *trustpoint-name* keyword and argument that is used during the Transport Layer Security (TLS) handshake that corresponds to the remote device address.
dial-peer cor custom	Specifies that named class of restrictions (COR) apply to dial peers.
dial-peer cor list	Defines a class of restrictions (COR) list name.
disable-early-media 180	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Specifies which call treatment, early media or local ringback, is provided for 180 responses with 180 responses with Session Description Protocol (SDP).
dspfarm profile	Enters DSP farm profile configuration mode and defines a profile for DSP farm services.

Command	Description
dtmf-interworking	Enables a delay between the dtmf-digit begin and dtmf-digit end events in the RFC 2833 packets sent from CUBE, and generates RFC 4733 compliance RTP Named Telephony Event (NTE) packets from CUBE.
early-media update block	Blocks the UPDATE requests with the Session Description Protocol (SDP) in an early dialog.
early-offer	Forces CUBE to send a SIP invite with Early Offer on the Out Leg.
emergency	Configures a list of emergency numbers.
error-code-override	Configures the SIP error code to be used at the dial peer.
error-passthru	Enables the passage of error messages from the incoming SIP leg to the outgoing SIP leg.
g729-annexb override	Configures the settings for G.729 codec interoperability and overrides the default value if the annexb attribute is not present.
gcid	Enables Global Call ID (GCID) for every call on an outbound leg of a VoIP dial peer for a SIP endpoint.
gw-accounting	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Enables an accounting method for collecting call detail records (CDRs).
handle-replaces	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Configures a Cisco IOS device to handle SIP INVITE with Replaces header messages at the SIP protocol level.
header-passing	Enables the passing of headers to and from SIP INVITE, SUBSCRIBE, and NOTIFY messages.
host-registrar	Populates the sip-ua registrar domain name or IP address value in the host portion of the diversion header and redirects the contact header of the 302 response.
http client connection idle timeout	Sets the number of seconds for which the HTTP client waits before terminating an idle connection.
http client connection persistent	Enables HTTP persistent connections so that multiple files can be loaded by using the same connection.
http client connection timeout	Sets the number of seconds for which the HTTP client waits for a server to establish a connection before abandoning its connection attempt.
ip qos dscp	Configures the DSCP value for QoS.

Command	Description
localhost	Globally configures CUBE to substitute a DNS hostname or domain as the localhost name in place of the physical IP address in the From, Call-ID, and Remote-Party-ID headers in outgoing messages.
max-conn	Specifies the maximum number of incoming or outgoing connections for a particular VoIP dial peer.
max-forwards	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Globally sets the maximum number of hops, that is, proxy or redirect servers that can forward the SIP request.
media	Enables media packets to pass directly between endpoints without the intervention of CUBE, and enables signaling services.
media disable-detailed-stats	Disables the collection of detailed call statistics.
media profile asp	Creates a media profile to configure acoustic shock-protection parameters.
media profile nr	Creates a media profile to configure noise-reduction parameters.
media profile stream-service	Enables stream service on CUBE.
media profile video	Creates a media profile video.
media-address voice-vrf	Associates an RTP port range with VRF.
media-inactivity-criteria	Specifies the mechanism for detecting media inactivity (silence) on a voice call.
midcall-signaling	Configures the method that is used for signaling messages.
min-se	Changes the minimum session expiration (Min-SE) header value for all the calls that use the SIP session timer.
nat	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Uses SIP Network Address Translation (NAT) global configuration.
nat media-keepalive	Enables media keepalive packet transmission for the specified interval of time.
notify redirect	Enables application handling of redirect requests for all VoIP dial peers.
notify ignore substate	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Specifies Ignoring the Subscription-State header in a Notify message.

Command	Description
notify telephone-event	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Configures the maximum interval between two consecutive NOTIFY messages for a particular telephone event.
num-exp	Defines how to expand a telephone extension number into a particular destination pattern.
options-ping	Enables in-dialog options.
outbound-proxy	Configures a SIP outbound proxy for outgoing SIP messages globally.
pass-thru content	Enables the pass-through of SDP from in-leg to the out-leg.
permit hostname	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Stores hostnames used during validation of initial incoming INVITE messages.
privacy	Sets privacy support at the global level as defined in RFC 3323.
privacy-policy	Configures the privacy header policy options at the global level.
progress_ind	Configures an outbound dial peer on a CUBE to override and remove or replace the default progress indicator in specified call messages.
protocol mode	Configures the Cisco IOS SIP stack.
random-contact	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Populates an outgoing INVITE message with random-contact information instead of clear-contact information.
reason-header override	Enables cause code passing from one SIP leg to another.
redirect ip2ip	Redirects SIP phone calls to SIP phone calls globally on a gateway.
redirection	Enables the handling of 3*xx* redirect messages
referto-passing	Disables dial peer lookup and modification of the Refer-To header when the CUBE passes across a REFER message during a call transfer.
registrar	Enables SIP gateways to register E.164 numbers on behalf of analog telephone voice ports (FXS), IP phone virtual voice ports (EFXS), and SCCP phones with an external SIP proxy or SIP registrar.
rel1xx	Enables SIP provisional responses (other than 100 Trying) to be sent reliably to the remote SIP endpoint.
remote-party-id	Enables translation of the Remote-Party-ID SIP header.

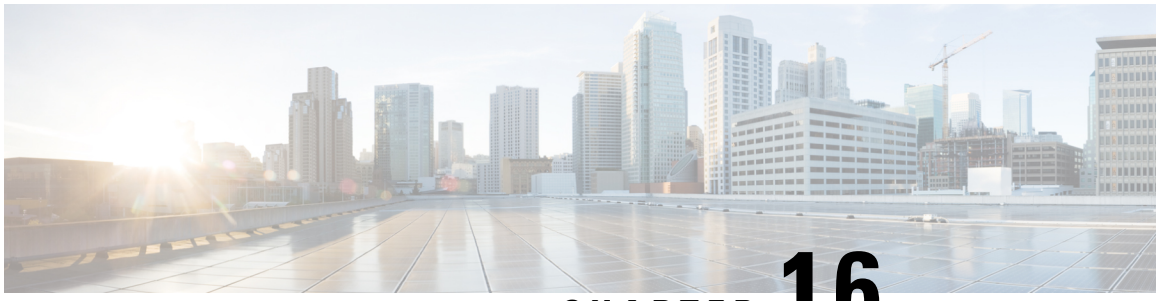
Command	Description
requri-passing	Enables pass-through of the host part of the Request-URI and To SIP headers.
retry bye	Configures the number of times that a BYE request is retransmitted to the other user agent.
retry invite	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Configures the number of times that a SIP INVITE request is retransmitted to the other user agent.
rtcp all-pass-through	Passes through all the RTCP packets in the datapath.
rtcp keepalive	Configures RTCP keepalive report generation and generates RTCP keepalive packets.
rtp payload-type	Identifies the payload type of an RTP packet.
rtp-media-loop count	Configures the number of media loops before RTP voice and video media packets are dropped.
rtp-port	Configures the real-time protocol range.
rtp-ssrc multiplex	Multiplexes RTCP packets with RTP packets and sends multiple synchronization source in RTP headers (SSRCs) in an RTP session.
secure-ciphersuite	Configures the cipher suites (encryption algorithms) to be used for encryption over HTTPS for a WebSocket connection in CUBE.
session refresh	Enables SIP session refresh globally.
session transport	Configures a VoIP dial peer to use TCP or UDP as the underlying transport layer protocol for SIP messages.
set pstn-cause	Maps an incoming PSTN cause code to a SIP error status code.
set sip-status	Maps an incoming SIP error status code to a PSTN cause code.
signaling forward	Configures global settings for transparent tunneling of QSIG, Q.931, H.225, and ISUP messages.
silent discard untrusted	Discards SIP requests from untrusted sources in an incoming SIP trunk.
sip-server	Configures a network address for the SIP server interface.
srtp	Specifies that SRTP be used to enable secure calls and call fallback.
srtp negotiate	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Enables the Cisco IOS Session Initiation Protocol (SIP) gateway to accept and send a Real-Time Transport Protocol (RTP) Audio/Video Profile (AVP) at the global configuration level.

Command	Description
stun	Enters STUN configuration mode for configuring firewall traversal parameters.
stun flowdata shared-secret	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Configures a secret shared on a call control agent.
stun usage firewall-traversal flowdata	Enables firewall traversal using STUN.
supplementary-service media-renegotiate	Globally enables midcall media renegotiation for supplementary services.
timers	Configures SIP-signaling timers.
transport	Configures the SIP user agent (gateway) for SIP signaling messages in inbound calls through the SIP TCP, TLS over TCP, or UDP socket. This command supports TLS version 1.3 and all associated ciphers.
uc secure-wsapi	Configures a secure Cisco Unified Communication IOS services environment for a specific application.
uc wsapi	Configures a nonsecure Cisco Unified Communication IOS services environment for a specific application.
update-callerid	Enables sending updates for caller IDs.
url (SIP)	Configures URLs to either the SIP, SIP secure (SIPS), or telephone (TEL) format for your VoIP SIP calls.
vad	Enables VAD for calls using a specific dial peer.
video codec	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a.
voice cause code	Sets the internal Q850 cause code mapping for, voice and enters voice cause configuration mode.
voice class codec	Enters voice-class configuration mode and assigns an identification tag number for a codec voice class.
voice class dpg	Creates a dial-peer group for grouping multiple outbound dial peers.
voice class e164-pattern-map	Creates an E.164 pattern map that specifies multiple destination E.164 patterns in a dial peer.
voice class media	Configures media control parameters for voice.
voice class server-group	Enters voice-class configuration mode and configures server groups (groups of IPv4 and IPv6 addresses) that can be referenced from an outbound SIP dial peer.

Command	Description
voice-class sip options-keepalive	Monitors connectivity between CUBE VoIP dial peers and SIP servers.
voice class sip-copylist	Configures a list of entities to be sent to the peer call leg.
voice class sip-event-list	Configures a list of SIP events to be passed through.
voice class sip-hdr-passthrulist	Configures a list of headers to be passed through the route string.
voice-class sip nat media-keepalive	Configures media keepalive to enable media keepalive packets to be transmitted for the interval specified.

voice class sip-profiles	Configures SIP profiles for a voice class.
	Configuring a sip profile, **request REGISTER sip-header Authorization modify "550\","[550@dl.ims.airtel.in|mailto:550@dl.ims.airtel.in]"**, on a device throws a warning message:
	`Device# show run`
	`sec sip-profiles voice class sip-profiles 4 rule 2`
	`request REGISTER sip-header Authorization modify`
	`"550\","`
	`"[550@dl.ims.airtel.in|mailto:550@dl.ims.airtel.in]""`

voice class srtp-crypto	Enters voice class configuration mode and assigns an identification tag for an **srtp-crypto voice class** command.
voice class uri	Creates or modifies a voice class for matching dial peers to a SIP or TEL URI.
voice class tls-cipher	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Configures an ordered set of TLS cipher suites.
voice class tls-profile	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Enables voice class configuration mode, and assigns an identification tag for a TLS profile.
voice iec syslog	Enables viewing of internal error codes as they are encountered in real time.
voice statistics iec	Enables collection of internal error code statistics.
xfer target	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a. Routes the INVITE to the refer-to destination in the REFER consume case. The routing decision is made based on the xfer target destination.



CHAPTER 16

Class-Map Commands

- class-map, on page 181
- match qos-group, on page 183
- pass, on page 184

class-map

To create a class map to be used for matching packets to a specified class and to enter QoS class-map configuration mode, use the **class-map** command in global configuration mode. To remove an existing class map from a device, use the **no** form of this command.

class-map { [**type inspect match-all**] | [**match-any**] } *class-map-name*
no class-map { [**type inspect match-all**] | [**match-any**] }

Syntax Description

type inspect	(Optional) Specifies the class-map type as inspect.
match-all	(Optional) Determines how packets are evaluated when multiple match criteria exist. Matches statements under this class map based on the logical AND function. A packet must match all statements to be accepted. If you do not specify the **match-all** or **match-any** keyword, the default keyword used is **match-all**.
match-any	(Optional) Determines how packets are evaluated when multiple match criteria exist. Matches statements under this class map based on the logical OR function. A packet must match any of the match statements to be accepted. If you do not specify the **match-any** or **match-all** keyword, the default keyword is used **match-all**.
class-map-name	Name of the class for the class map. The class name is used for both the class map and to configure a policy for the class in the policy map. **Note** You can enter the value for the *class-map-name* argument within quotation marks. The software does not accept spaces in a class map name entered without quotation marks.

Command Default

A class map is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `class-map` command.

Examples

```
class-map match-any BestEffort
  match qos-group 3
 !
 class-map match-any Bulk
  match qos-group 4
 !
 class-map match-any Critical
  match qos-group 1
 !
 class-map match-any Critical-Low
  match qos-group 2
 !
 class-map match-any BULK
  match qos-group 2
 !
 class-map match-any CONTROL-SIGNALING
  match qos-group 4
 !
 class-map match-any CRITICAL-DATA
  match qos-group 1
 !
 class-map match-any Default
  match qos-group 5
 !
 class-map match-any INTERACTIVE-VIDEO
  match qos-group 3
 !
 class-map match-any LLQ
  match qos-group 0
 !
 class-map match-any Queue0
  match qos-group 0
 !
 class-map match-any Queue1
  match qos-group 1
 !
 class-map match-any Queue2
  match qos-group 2
 !
 class-map match-any Queue3
  match qos-group 3
 !
 class-map match-any Queue4
  match qos-group 4
 !
 class-map match-any Queue5
  match qos-group 5
 !
 class-map type inspect match-all cmap
  match access-group name cmap
 !
 class-map match-any Queue4
  match qos-group 0
 !
```

The following example configures the match criterion for a class map on the basis of a specified protocol for zone based policy firewall:

```
class-map match-any aa1-cm0_
match protocol test
match protocol mpeg2-ts
!
```

match qos-group

To identify a specific quality of service (QoS) group value as a match criterion, use the **match qos-group** command in class-map configuration or policy inline configuration mode. To remove a specific QoS group value from a class map, use the **no** form of this command.

match qos-group *qos-group-value*
no match qos-group *qos-group-value*

Syntax Description

qos-group-value	The exact value from 0 to 99 used to identify a QoS group value.

Command Default

No match criterion is specified.

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Examples

```
class-map match-any BestEffort
  match qos-group 3
 !
 class-map match-any Bulk
  match qos-group 4
 !
 class-map match-any Critical
  match qos-group 1
 !
 class-map match-any Critical-Low
  match qos-group 2
 !
 class-map match-any BULK
  match qos-group 2
 !
 class-map match-any CONTROL-SIGNALING
  match qos-group 4
 !
 class-map match-any CRITICAL-DATA
  match qos-group 1
 !
 class-map match-any Default
  match qos-group 5
```

```
!
class-map match-any INTERACTIVE-VIDEO
 match qos-group 3
!
class-map match-any LLQ
 match qos-group 0
!
class-map match-any Queue0
 match qos-group 0
!
class-map match-any Queue1
 match qos-group 1
!
class-map match-any Queue2
 match qos-group 2
!
class-map match-any Queue3
 match qos-group 3
!
class-map match-any Queue4
 match qos-group 4
!
class-map match-any Queue5
 match qos-group 5
!
```

pass

To allow packets to be sent to the router without being inspected, use the **pass** command in policy-map-class configuration mode.

pass log

Command Default

No default behavior or values.

Command Modes

Policy-map-class configuration mode (config-pmap-c)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

The zone-based firewall feature can be enabled on a Cisco IOS XE Catalyst SD-WAN devices for inspecting traffic exchange between multiple service VPNs. **policy-map type inspect** command can be used to create a policy-map under which class or class type inspect command can be called for taking further actions on the traffic of interest.

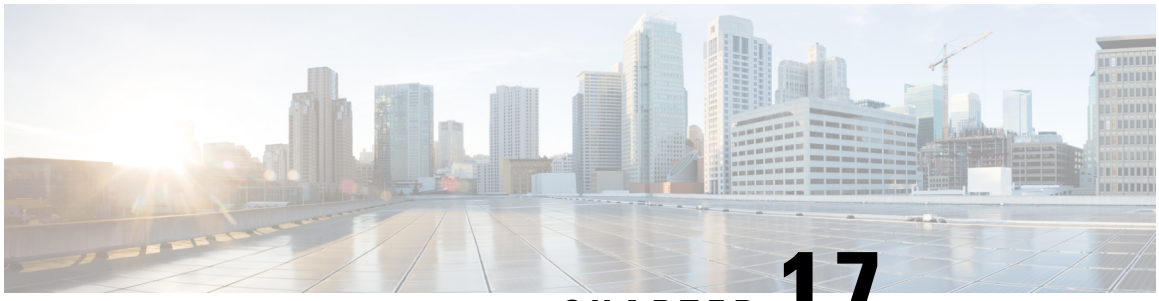
Examples

The following example shows how to create a policy-map type inspect fw_policy1. Inside this policy-map, a class of class type inspect cmap_1 has been called. Inside the class type inspect, pass log command can be called to not drop or inspect packets for the desired class.

```
Device(config)# policy-map type inspect fw_policy1
Device(config-pmap)# class type inspect cmap_1
Device(config-pmap-c)# pass log
```

Related Commands

Command	Description
policy-map type inspect *policy-name*	Creates a Layer 3 or Layer 4 inspect type policy map.
class type inspect *class-name*	Specifies the traffic class on which an action is to be performed.
log	Logs the firewall activity for an inspect parameter map.



CHAPTER 17

Cloud OnRamp for SaaS Commands

- probe-path load-balance-dia latency-variance, on page 187
- probe-path load-balance-dia loss-variance, on page 189
- probe-path load-balance-dia source-ip-hash, on page 191
- probe saas-app, on page 192
- probe saas-app webex, on page 193

probe-path load-balance-dia latency-variance

To configure the latency variance for Cloud onRamp for SaaS load balancing, use the **probe-path load-balance-dia latency-variance** command in global configuration mode. To disable Cloud onRamp for SaaS load balancing, use the **no** form of the command.

probe-path load-balance-dia latency-variance *latency-variance*

no probe-path load-balance-dia latency-variance

Syntax Description

latency-variance	To use another interface for load balancing, the latency value of the interface cannot vary from the latency of the best path interface by more than this number of milliseconds. You can configure a smaller value to restrict load balancing only to interfaces with a latency value very close to that of the best path interface, or you can configure a larger value to be more inclusive of interfaces that might have a higher latency than the best path interface. For example, if the best path interface has a latency of 5 milliseconds, and the *latency-variance* is set to 15, then another interface can be used for load balancing only if its latency is no more than 20 milliseconds. Range: 1 to 1000 (milliseconds) Default: 50

Command Default

50 milliseconds

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	This command was introduced.

Usage Guidelines

Note We recommend configuring Cloud onRamp for SaaS load balancing using Cisco SD-WAN Manager, not by CLI.

By default, Cloud onRamp for SaaS load balancing is disabled. Any of the following commands can enable Cloud onRamp for SaaS load balancing:

- **probe-path load-balance-dia latency-variance**
- **probe-path load-balance-dia loss-variance**
- **probe-path load-balance-dia source-ip-hash**

Using the **no** form of each of the commands disables Cloud onRamp for SaaS load balancing after it has been enabled:

- **no probe-path load-balance-dia latency-variance**
- **no probe-path load-balance-dia loss-variance**
- **no probe-path load-balance-dia source-ip-hash**

After determining the best path interface for a cloud application, Cloud onRamp for SaaS compares the performance statistics for other interfaces. To use another interface for load balancing, the following must be true:

- The packet loss value of the interface must be within a configured percentage of the value for the best path interface. See the **probe-path load-balance-dia loss-variance** command.
- The latency value of the interface cannot vary from the latency of the best path interface by more than a configured number of milliseconds (configured by this command).

Example

The following example configures a latency variance of 50 milliseconds.

```
Device(config)# probe-path load-balance-dia latency-variance 50
```

Example

The **show full-configuration probe-path load-balance-dia** command displays the currently configured parameters for Cloud onRamp for SaaS load balancing.

```
Device(config)# show full-configuration probe-path load-balance-dia
probe-path load-balance-dia latency-variance 50
probe-path load-balance-dia loss-variance 30
probe-path load-balance-dia source-ip-hash false
```

Example

The **no** form of each of the following commands disables Cloud onRamp for SaaS load balancing.

```
Device(config)# no probe-path load-balance-dia latency-variance
Device(config)# no probe-path load-balance-dia loss-variance
Device(config)# no probe-path load-balance-dia source-ip-hash
```

probe-path load-balance-dia loss-variance

To configure the packet loss variance for Cloud onRamp for SaaS load balancing, use the **probe-path load-balance-dia loss-variance** command in global configuration mode. To disable Cloud onRamp for SaaS load balancing, use the **no** form of the command.

probe-path load-balance-dia loss-variance *loss-variance*

no probe-path load-balance-dia loss-variance

Syntax Description

loss-variance	To use another interface for load balancing, the packet loss value of the interface must be within the percentage configured with *loss-variance* , compared with the value for the best path interface. You can configure a smaller value to restrict load balancing only to interfaces with a packet loss value very close to that of the best path interface, or you can configure a larger value to be more inclusive of interfaces that might have a higher packet loss than the best path interface. For example, if the best path interface has a packet loss value of 2% and the *loss-variance* value is 10, then another interface can be used for load balancing only if its packet loss value is no more than 12%. Range: 1 to 100 (percent) Default: 10

Command Default

10

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	This command was introduced.

Usage Guidelines

Note We recommend configuring Cloud onRamp for SaaS load balancing using Cisco SD-WAN Manager, not by CLI.

By default, Cloud onRamp for SaaS load balancing is disabled. Any of the following commands can enable Cloud onRamp for SaaS load balancing:

- **probe-path load-balance-dia latency-variance**
- **probe-path load-balance-dia loss-variance**
- **probe-path load-balance-dia source-ip-hash**

Using the **no** form of each of the commands disables Cloud onRamp for SaaS load balancing after it has been enabled:

- **no probe-path load-balance-dia latency-variance**
- **no probe-path load-balance-dia loss-variance**
- **no probe-path load-balance-dia source-ip-hash**

After determining the best path interface for a cloud application, Cloud onRamp for SaaS compares the performance statistics for other interfaces. To use another interface for load balancing, the following must be true:

- The packet loss value of the interface must be within a configured percentage of the value for the best path interface (configured by this command).
- The latency value of the interface cannot vary from the latency of the best path interface by more than a configured number of milliseconds. See the **probe-path load-balance-dia latency-variance** command.

Example

The following example configures a packet loss variance of 30 percent.

```
Device(config)# probe-path load-balance-dia loss-variance 30
```

Example

The **show full-configuration probe-path load-balance-dia** command displays the currently configured parameters for Cloud onRamp for SaaS load balancing.

```
Device(config)# show full-configuration probe-path load-balance-dia
probe-path load-balance-dia latency-variance 50
probe-path load-balance-dia loss-variance 30
probe-path load-balance-dia source-ip-hash false
```

Example

The **no** form of each of the following commands disables Cloud onRamp for SaaS load balancing.

```
Device(config)# no probe-path load-balance-dia latency-variance
Device(config)# no probe-path load-balance-dia loss-variance
Device(config)# no probe-path load-balance-dia source-ip-hash
```

probe-path load-balance-dia source-ip-hash

To ensure that all traffic from a single host uses a single interface, when using Cloud onRamp for SaaS load balancing, use the **probe-path load-balance-dia source-ip-hash** command in global configuration mode. To disable this option, use the **no** form of this command.

probe-path load-balance-dia source-ip-hash

no probe-path load-balance-dia source-ip-hash

Command Default Disabled

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	This command was introduced.

Usage Guidelines

Note We recommend configuring Cloud onRamp for SaaS load balancing using Cisco SD-WAN Manager, not by CLI.

By default, Cloud onRamp for SaaS load balancing is disabled. Any of the following commands can enable Cloud onRamp for SaaS load balancing:

- **probe-path load-balance-dia latency-variance**
- **probe-path load-balance-dia loss-variance**
- **probe-path load-balance-dia source-ip-hash**

Using the **no** form of each of the commands disables Cloud onRamp for SaaS load balancing after it has been enabled:

- **no probe-path load-balance-dia latency-variance**
- **no probe-path load-balance-dia loss-variance**
- **no probe-path load-balance-dia source-ip-hash**

Cloud onRamp for SaaS determines the best network path for each type of cloud traffic. However, if multiple direct internet access (DIA) interfaces on a WAN edge device at a branch site provide acceptable performance for a cloud application, Cloud onRamp for SaaS can employ load balancing across multiple interfaces to further improve performance. When you enable load balancing across multiple interfaces of a WAN edge devices, load balancing is enabled for all cloud applications that are managed by Cloud onRamp for SaaS.

If you want all traffic from a single host, such as a device within your network, to use a single interface (not load balancing), you can enable this option. For example, you may want DNS and application traffic from a

device to use the same interface. Use the **probe-path load-balance-dia source-ip-hash** command to configure this.

Example

```
Device(config)# probe-path load-balance-dia source-ip-hash
```

Example

The **show full-configuration probe-path load-balance-dia** command displays the currently configured parameters for Cloud onRamp for SaaS load balancing.

```
Device(config)# show full-configuration probe-path load-balance-dia
probe-path load-balance-dia latency-variance 50
probe-path load-balance-dia loss-variance 30
probe-path load-balance-dia source-ip-hash false
```

Example

Executing the **no** form of each of the following commands disables Cloud onRamp for SaaS load balancing.

```
Device(config)# no probe-path load-balance-dia latency-variance
Device(config)# no probe-path load-balance-dia loss-variance
Device(config)# no probe-path load-balance-dia source-ip-hash
```

probe saas-app

To define a SaaS application list for Cloud onRamp for SaaS, use the **probe saas-app** command in global configuration mode. To remove a SaaS application list, use the **no** form of the command.

Note We do not recommend using this command. We recommend using Cisco SD-WAN Manager to configure this feature. Configuring Cloud onRamp for SaaS features using CLI commands causes devices to be out of synchronization with Cisco SD-WAN Manager.

probe saas-app *applist-name application*
[*application ...*]
{ **endpoint-ip** *ip-address* | **endpoint-fqdn** *fqdn* | **endpoint-url** *url* }

no probe saas-app *applist-name*

Syntax Description

applist-name	Name of the SaaS application list.
application	Applications to include in the SaaS application list. Minimum number of applications: 1 Maximum number of applications: 8

endpoint-ip *ip-address*	IP address of the application server to probe. Cloud onRamp for SaaS probes the server using port 80.
endpoint-fqdn *fqdn*	Fully qualified domain name of the application server to probe. Cloud onRamp for SaaS probes the server using port 80.
endpoint-url *url*	A URL using HTTP or HTTPS of the application server to probe. Cloud onRamp for SaaS probes the server using port 80 or port 443, depending on the URL provided.

Command Default

By default, no application list is defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	This command was introduced.

Example

The following example creates a SaaS application list called example-apps that includes two applications (example-audio and example-video) and specifies www.example.com as the endpoint for probing to find the best path.

```
probe saas-app example-apps
  app example-audio
  app example-video
  endpoint-fqdn www.example.com
```

probe saas-app webex

To enable Cloud onRamp for SaaS to determine the best path for network traffic for Webex, use the **probe saas-app webex** command in global configuration mode.

Note We do not recommend using this command. It requires an understanding of Webex server information and knowledge of how to configure region-name, region-id, and endpoint-fqdn. In addition, using this command can cause a device to go out of synchronization with the configuration of Cloud onRamp for SaaS by Cisco SD-WAN Manager.

probe saas-app webex region *region-name* **id** *region-id* **endpoint-fqdn** *server-fqdn*

Syntax Description

region *region-name*	Region of the Webex server.
id *region-id*	Region ID of the Webex server.
endpoint-fqdn *server-fqdn*	Fully qualified domain name of the Webex server.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

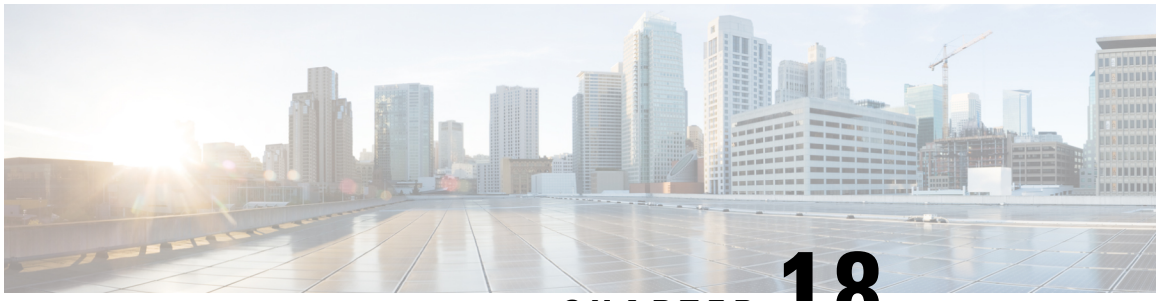
Note We do not recommend using this command. It requires an understanding of Webex server information and knowledge of how to regions and ID's. In addition, using this command can cause a device to go out of synchronization with the configuration of Cloud onRamp for SaaS by Cisco SD-WAN Manager.

Examples

The following example configures two webex servers.

```
probe
saas-app webex
  region ap-east-1
   id 231
   endpoint-fqdn  pinger.ap-east-1.net.infra.webex.com

  !
  region ap-northeast-1
   id 221
   endpoint-fqdn  pinger.ap-northeast-1.net.infra.webex.com
  !
```



CHAPTER 18

Crypto Commands

- aaa authorization (IKEv2 profile), on page 196
- address (IKEv2 keyring), on page 197
- authentication (IKEv2 profile), on page 198
- config-exchange, on page 199
- crypto ikev2 authorization policy, on page 200
- crypto ikev2 diagnose, on page 200
- crypto ikev2 keyring, on page 201
- crypto ikev2 limit, on page 202
- crypto ikev2 policy, on page 203
- crypto ikev2 profile, on page 203
- crypto ikev2 proposal, on page 204
- crypto ipsec profile, on page 205
- crypto ipsec transform-set, on page 206
- crypto isakmp aggressive-mode disable, on page 207
- crypto pki import, on page 207
- crypto pki trustpoint, on page 208
- encryption (IKEv2 proposal), on page 209
- enrollment selfsigned, on page 210
- group (IKEv2 proposal), on page 210
- integrity, on page 211
- keyring (IKEv2 profile), on page 211
- lifetime (IKEv2 profile), on page 212
- match identity remote, on page 213
- mode (IPSec), on page 214
- multi-tenancy, on page 215
- parameter-map type inspect-global, on page 216
- peer, on page 217
- pre-shared-key, on page 218
- proposal, on page 219
- revocation-check, on page 220
- set ikev2-profile, on page 220
- set pfs, on page 221
- set security-association lifetime, on page 223

- set security-association replay window-size, on page 224
- set transform-set, on page 224
- subject-name, on page 225

aaa authorization (IKEv2 profile)

To specify the authentication, authorization, and accounting (AAA) authorization for a local or external group policy, use the **aaa authorization** command in IKEv2 profile configuration mode. To remove the AAA authorization, use the **no** form of this command.

aaa authorization { **group** { **cert list** | **eap list** | **psk list** } | **user** { **cert list** | **eap list** | **psk list** } { *aaa-listname* | [*aaa-username* | [**local**] | **name-mangler** *mangler-name*] | [**password** *password*] } }
no aaa authorization { **group** { **cert list** | **eap list** | **psk list** } | **user** { **cert list** | **eap list** | **psk list** } { *aaa-listname* | [*aaa-username* | [**local**] | **name-mangler** *mangler-name*] | [**password** *password*] } }

Syntax Description

group	Specifies the AAA authorization for local or external group policy.
local	(Optional) Specifies the authorization policy that is used through a local method.
user	Specifies the AAA authorization for each user policy.
cert	Specifies the AAA method list that is used when the remote authentication method is certificate based.
eap	Specifies the AAA method list that is used when the remote authentication method is Extensible Authentication Protocol (EAP).
psk	Specifies the AAA method list that is used when the remote authentication method is preshared key.
list	Specifies the AAA method list for the remote authentication method.
aaa-listname	The AAA list name.
aaa-username	The AAA username.
name-mangler *mangler-name*	Derives the name mangler from the **crypto ikev2 name-mangler** command.
password *password*	Specifies the AAA password. This *password* argument defines the following values: • **0**—Specifies that the password is unencrypted. • **6**—Specifies that the password is encrypted. • *password*—Specifies an unencrypted user password.

Command Default

AAA authorization is not specified.

Command Modes IKEv2 profile configuration (config-ikev2-profile)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines For usage guidelines, see the Cisco IOS XE aaa authorization (IKEv2 profile) command.

Examples The following example shows how to configure the AAA authorization for a local group policy.

```
\
Router(config)# crypto ikev2 profile if-ipsec256-ikev2-profile
Router(config-ikev2-profile)# aaa authorization group psk list default li_policy
```

address (IKEv2 keyring)

To specify an IPv4 address or the range of the peer in an Internet Key Exchange Version 2 (IKEv2) keyring, use the **address** command in IKEv2 keyring peer configuration mode. To remove the IP address, use the **no** form of this command.

address *ipv4-address*
no address

Syntax Description

ipv4-address	IPv4 address of the remote peer.

Command Default There is no default IP address.

Command Modes IKEv2 keyring peer configuration (config-ikev2-keyring-peer)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines For usage guidelines, see the Cisco IOS XE address (IKEv2 keyring) command.

Examples The following examples show how to specify the preshared key of an IP Security (IPsec) peer:

```
Router(config)#  crypto ikev2 keyring if-ipsec256-ikev2-keyring
Router(config-ikev2-keyring)# peer if-ipsec256-ikev2-keyring-peer
Router(config-ikev2-keyring-peer)# address 172.16.93.1
Router(config-ikev2-keyring-peer)# pre-shared-key cisco123
```

authentication (IKEv2 profile)

To specify the local and remote authentication methods in an Internet Key Exchange Version 2 (IKEv2) profile, use the **authentication** command in IKEv2 profile configuration mode. To delete the authentication method, use the **no** form of this command.

authentication { **local** { **rsa-sig** | **pre-share** [**key**] | **ecdsa-sig** } | **remote** { **anyconnect-eap** | **rsa-sig** | **pre-share** [**key**] } }
no authentication { **local** { **rsa-sig** | **pre-share** [**key**] | **ecdsa-sig** } | **remote** { **anyconnect-eap** | **rsa-sig** | **pre-share** [**key**] } }

Syntax Description

local	Specifies the local authentication method.
rsa-sig	Specifies Rivest, Shamir, and Adelman (RSA) signature as the authentication method. As described in the usage guidelines, the **rsa-sig-deprecated** command is available for specific mixed-release scenarios.
pre-share	Specifies preshared key as the authentication method. As described in the usage guidelines, the **pre-share-deprecated** command is available for specific mixed-release scenarios.
key	Specifies a preshared key.
ecdsa-sig	Specifies Elliptic Curve Digital Signature Algorithm (ECDSA) signature (ECDSA-sig) as the authentication method. As described in the usage guidelines, the **ecdsa-sig-deprecated** command is available for specific mixed-release scenarios.
anyconnect-eap	Specifies Extensible Authentication Protocol (EAP) as the authentication method.
remote	Specifies the remote authentication method.

Command Default

The default local and remote authentication method is not configured.

Command Modes

IKEv2 profile configuration (crypto-ikev2-profile)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.
Cisco IOS XE Catalyst SD-WAN Release 26.2.1	Added **-deprecated** versions of a few keywords, as noted in the keyword descriptions, to address specific mixed-release scenarios. The usage guidelines describe the details of the mixed-release scenarios that require the **-deprecated** keywords.

Usage Guidelines

For basic usage guidelines, see the Cisco IOS XE authentication (IKEv2 profile) command.

Usage Guidelines

Mixed releases

There is a scenario of a mixed-release network, with SD-WAN Manager operating with release 26.2.x or later, and some devices in the network using a Cisco IOS XE Release earlier than 26.2.1. In this mixed-release scenario, there is a specific requirement if you are including one of these commands in a configuration:

```
authentication local pre-share
authentication local dynamic
authentication local rsa-sig
authentication local ecdsa-sig
```

If using one these commands, then also include the **-deprecated** version of the command in the configuration. Here's an example for the **pre-share** keyword, showing both versions of the command:

```
crypto ikev2 profile IKEV2-PSK-PROFILE
  authentication local pre-share
  authentication local pre-share-deprecated
exit
```

Examples

The following example shows how to specify an authentication method in an IKEv2 profile:

```
Device(config)# crypto ikev2 profile if-ipsec256-ikev2-profile
Device(config-ikev2-profile)# aaa authorization group psk list default li_policy
Device(config-ikev2-profile)# authentication local pre-share
Device(config-ikev2-profile)# authentication remote pre-share
Device(config-ikev2-profile)# no config-exchange request
Device(config-ikev2-profile)# keyring local if-ipsec256-ikev2-keyring
Device(config-ikev2-profile)# lifetime 86400
Device(config-ikev2-profile)# match identity remote address 172.16.93.2
!
```

In the above example, the profile if-ipsec256-ikev2-profile specifies preshare as the local authentication method and as the remote authentication method that use keyring if-ipsec256-ikev2-keyring.

config-exchange

To enable the configuration exchange options, use the **config-exchange** command in IKEv2 profile configuration mode. To disable sending, use the **no** form of this command.

config-exchange {**request** | **set** {**accept** | **send**}}
no config-exchange {**request** | **set** {**accept** | **send**}}

Syntax Description

request	Enables configuration exchange request.
set	Enables configuration exchange request set options.
accept	Accepts configuration exchange request set.
send	Enables sending of configuration exchange set.

Command Default

The configuration exchange options is enabled by default.

Command Modes

IKEv2 profile configuration (config-ikev2-profile)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE config-exchange command.

Examples

The following example show how to set the acceptance of configuration exchange request for the IKEv2 profile "if-ipsec256-ikev2-profile":

```
Router(config)# crypto ikev2 profile if-ipsec256-ikev2-profile
Router(config-ikev2-profile)# config-exchange set accept
```

crypto ikev2 authorization policy

To configure an IKEv2 authorization policy, use the **crypto ikev2 authorization policy** command in global configuration mode. To remove this command and all associated subcommands from your configuration, use the **no** form of this command.

crypto ikev2 authorization policy *policy-name*
no crypto ikev2 authorization policy *policy-name*

Syntax Description

policy-name	Group definition that identifies which policy is enforced for users.

Command Default

None.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE crypto ikev2 authorization policy command.

Examples

In this example, the policy is enforced for users that matches the group name "li_policy."

```
crypto ikev2 authorization policy
li_policy
  exit
```

crypto ikev2 diagnose

To enable Internet Key Exchange Version 2 (IKEv2) error diagnostics, use the **crypto ikev2 diagnose** command in global configuration mode. To disable the error diagnostics, use the **no** form of this command.

crypto ikev2 diagnose error *number*
no crypto ikev2 diagnose error

Syntax Description

error	Enables the IKEv2 error path tracing.
number	Specifies the maximum number of errors allowed in the exit path entry. The range is 1 to 1000.

Command Default

IKEv2 error diagnostics is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE crypto ikev2 diagnose command.

Examples

The following example shows that error diagnostics is disabled:

```
Router(config)# no crypto ikev2 diagnose error
```

crypto ikev2 keyring

To configure an Internet Key Exchange version 2 (IKEv2) key ring, use the **crypto ikev2 keyring** command in the global configuration mode. To delete an IKEv2 keyring, use the **no** form of this command.

crypto ikev2 keyring *keyring-name*
no crypto ikev2 keyring *keyring-name*

Syntax Description

keyring-name	Name of the keyring.

Command Default

There is no default key ring.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE crypto ikev2 keyring command.

Examples

The following example shows how to configure a keyring:

```
Router(config)# crypto ikev2 keyring if-ipsec256-ikev2-keyring
Router(config-ikev2-keyring)# peer if-ipsec256-ikev2-keyring-peer
Router(config-ikev2-keyring-peer)# address 172.16.93.1
Router(config-ikev2-keyring-peer)# pre-shared-key cisco123
!
!
```

crypto ikev2 limit

To configure the maximum number of active incoming or outgoing connections from a device, use the **crypto ikev2 limit** command in global configuration mode.

max-in-negotiation-sa *max-connections*
{ **incoming** | **outgoing** }

Syntax Description

max-connections **incoming**	Configure the maximum number of active incoming connections to a device. Limiting the number is useful for resource management, protecting the device CPU and crypto engine from overload or denial-of-service attacks. Range: 1 through 9999 Default: 40 for incoming
max-connections **outgoing**	Configure the maximum number of active outgoing connections from a device. Limiting the number is useful for resource management, protecting the device CPU and crypto engine from overload or denial-of-service attacks. Range: 1 through 9999 Default: 60

Command Default

Maximum outgoing connections: 60

Maximum incoming connections: 40

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 26.2.1	Changed default maximum outgoing connections from 400 to 60.

Usage Guidelines

If the device needs to support more than 60 outgoing connections, configure max-in-negotiation-sa maximum outgoing accordingly.

Example

This configures a device to support 100 outgoing connections.

```
Device#max-in-negotiation-sa 100 outgoing
```

Related commands

Command	Description
show crypto ikev2 stats	Displays IKEv2 statistics.

crypto ikev2 policy

To configure an Internet Key Exchange Version 2 (IKEv2) policy, use the **crypto ikev2 policy** command in global configuration mode. To delete a policy, use the **no** form of this command. To return the policy to its default value, use the **default** form of this command.

crypto ikev2 policy *name*
no crypto ikev2 policy *name*
default crypto ikev2 policy

Syntax Description

name	Name of the IKEv2 policy.

Command Default

A default IKEv2 policy is used only in the absence of any user-defined IKEv2 policy. The default IKEv2 policy will have the default IKEv2 proposal and will match all local addresses in a global VPN Routing and Forwarding (VRF).

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE crypto ikev2 policy command.

Examples

The following example show how to configure a policy:

```
Router(config)# crypto ikev2 policy policy1-global
Router(config-ikev2-policy)# proposal p1-global
```

crypto ikev2 profile

To configure an Internet Key Exchange Version 2 (IKEv2) profile, use the **crypto ikev2 profile** command in global configuration mode. To delete the profile, use the **no** form of this command.

crypto ikev2 profile *profile-name*
no crypto ikev2 profile *profile-name*

Syntax Description

profile-name	The name of the IKEv2 profile.

Command Default

There is no default IKEv2 profile. However, there are default values for some commands under the profile, such as lifetime.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE crypto ikev2 profilecommand.

Examples

The following example show an IKEv2 profile matched on a remote identity.

IKEv2 Profile Matched on Remote Identity

The following profile caters to peers that identify using a remote address and authenticate with pre-share. The local node authenticates with pre-share using keyring, if-ipsec256-ikev2-keyring.

```
Router(config)# crypto ikev2 profile if-ipsec256-ikev2-profile
Router(config-ikev2-profile)# aaa authorization group psk list default li_policy
Router(config-ikev2-profile)# authentication local pre-share
Router(config-ikev2-profile)# authentication remote pre-share
Router(config-ikev2-profile)# no config-exchange request
Router(config-ikev2-profile)# keyring local if-ipsec256-ikev2-keyring
Router(config-ikev2-profile)# lifetime 86400
Router(config-ikev2-profile)# match identity remote address 172.16.93.2
!
```

crypto ikev2 proposal

To configure an Internet Key Exchange Version 2 (IKEv2) proposal, use the **crypto ikev2 proposal** command in global configuration mode. To delete an IKEv2 proposal, use the **no** form of this command. To return the proposal to its default value, use the **default** form of this command.

crypto ikev2 proposal *name*
no crypto ikev2 proposal *name*
default crypto ikev2 proposal

Syntax Description

name	Name of the proposal. The proposals are attached to IKEv2 policies using the **proposal** command.

Command Default

The default IKEv2 proposal is used.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE crypto ikev2 proposal command.

Examples

The following example shows how to configure a proposal:

```
Device(config)# crypto ikev2 proposal p1-global
Device(config-ikev2-proposal)# encryption aes-cbc-128 aes-cbc-256
Device(config-ikev2-proposal)# group 14 15 16 2
Device(config-ikev2-proposal)# integrity sha1 sha256 sha384 sha512
!
```

crypto ipsec profile

To define the IP Security (IPsec) parameters that are to be used for IPsec encryption between two IPsec routers and to enter IPsec profile configuration mode, use the **crypto ipsec profile** command in global configuration mode. To delete an IPsec profile, use the **no** form of this command. To return the IPsec profile to its default value, use the **default** form of this command.

crypto ipsec profile *name*
no crypto ipsec profile *name*

Syntax Description

name	Profile name.

Command Default

The default IPsec profile is used.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE crypto ipsec profile command.

Examples

The following example shows how to configure a crypto map that uses an IPsec profile:

```
crypto ipsec profile if-ipsec256-ipsec-profile
 set ikev2-profile if-ipsec256-ikev2-profile
```

```
 set pfs group16
 set transform-set if-ipsec256-ikev2-transform
 set security-association lifetime kilobytes disable
 set security-association lifetime seconds 3600
 set security-association replay window-size 512
!
```

crypto ipsec transform-set

To define a transform set—an acceptable combination of security protocols and algorithms—use the **crypto ipsec transform-set** command in global configuration mode. To delete a transform set, use the **no** form of this command. To return the transform-set to its default value, use the **default** form of this command.

crypto ipsec transform-set *transform-set-name transform1* [*transform2*] [*transform3*] [*transform4*]
no crypto ipsec transform-set *transform-set-name*

Syntax Description

transform-set-name	Name of the transform set to create (or modify).
transform1 transform2 transform3 transform4	Type of transform set. You may specify up to four "transforms": one Authentication Header (AH), one Encapsulating Security Payload (ESP) encryption, one ESP authentication, and one compression. These transforms define the IP Security (IPSec) security protocols and algorithms. Accepted transform values are available in the usage guidelines.

Command Default

The default transform-set is used.

Command Modes

Global configuration

This command invokes the crypto transform configuration mode.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE crypto ipsec transform-set command.

Examples

The following example defines a transform set. The transform set will be used with an IPSec peer that supports the esp-gcm protocols.

```
Router (config)# crypto ipsec transform-set if-ipsec256-ikev2-transform esp-gcm 256
Router (cfg-crypto-trans)# mode tunnel
!
```

Examples

crypto isakmp aggressive-mode disable

To block all Internet Security Association and Key Management Protocol (ISAKMP) aggressive mode requests to and from a device, use the **crypto isakmp aggressive-mode disable** command in global configuration mode. To disable the blocking, use the **no** form of this command.

crypto isakmp aggressive-mode disable
no crypto isakmp aggressive-mode disable

Syntax Description

This command has no arguments or keywords.

Command Default

If this command is not configured, Cisco IOS software will attempt to process all incoming ISAKMP aggressive mode security association (SA) connections. In addition, if the device has been configured with the **crypto isakmp peer address** and the **set aggressive-mode password**or **set aggressive-mode client-endpoint**commands, the device will initiate aggressive mode if this command is not configured.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE crypto isakmp aggressive-mode disable command.

Examples

The following example shows that all aggressive mode requests to and from a device are blocked:

```
Router (config)# crypto isakmp aggressive-mode disable
```

crypto pki import

To import Rivest, Shamir, and Adleman (RSA) keys, use the **crypto pki import pkcs12 password** command in privileged EXEC mode. To remove any of the configured parameters, use the no form of this command

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE crypto pki import command.

Examples

In the following example, an RSA key pair that has been associated with the trustpoint named **test2** is to be imported:

```
Device# crypto pki import test2 pkcs12 bootflash:router1.p12 password cisco123
% Importing pkcs12...Reading file from bootflash:router1.p12
CRYPTO_PKI: Imported PKCS12 file successfully.
```

crypto pki trustpoint

To declare the trustpoint that your router should use, use the **crypto pki trustpoint** command in global configuration mode. To delete all identity information and certificates associated with the trustpoint, use the **no** form of this command.

crypto pki trustpoint *name* { **ca-check-strict** | **scepencrypt** | { **aes128** | **aes192** | **aes256** | **des_ede3** } }
no crypto pki trustpoint *name*

Syntax Description

name	Creates a name for the trustpoint. (If you previously declared the trustpoint and just want to update its characteristics, specify the name you previously created.)
ca-check-strict	If you enable this command, the peer will reject a CA certificate without basic constraints.
scepencrypt	Specifies the encryption method used by Simple Certificate Enrollment Protocol (SCEP) • **aes128**: Uses the AES-128-CBC encryption algorithm for SCEP. • **aes192** : Uses the AES-192-CBC encryption algorithm for SCEP. • **aes256**: Uses the AES-256-CBC encryption algorithm for SCEP. • **des_ede3**: Uses the Triple DES (3DES) encryption algorithm for SCEP.

Command Default

Your router does not recognize any trustpoints until you declare a trustpoint using this command.

Your router uses unique identifiers during communication with Online Certificate Status Protocol (OCSP) servers, as configured in your network.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.
Cisco IOS XE Catalyst SD-WAN Release 17.18.1a	The **ca-check-strict** was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE crypto pki trustpoint command.

Examples

The following example shows a self-signed certificate being designated for a trustpoint named local using the enrollment selfsigned subcommand of the crypto pki trustpoint command:

```
crypto pki trustpoint TP-self-signed-3865005142
enrollment selfsigned
```

The following example shows the **ca-check-strict** command being enabled:

```
Device (config)#crypto pki trustpoint ca
Device (ca- trustpoint)#
 CRYPTO_PKI: Creating trustpoint ca
 CRYPTO PKI: handle 1073741863 associated with trustpoint ca
Device (ca-trustpoint) #
 %PKI-6-TRUSTPOINT_CREATE: Trustpoint: ca created successfully
Device (ca-trustpoint)#ca
Device (ca-trustpoint)#ca-check-strict
```

encryption (IKEv2 proposal)

To specify one or more encryption algorithms for an Internet Key Exchange Version 2 (IKEv2) proposal, use the **encryption** command in IKEv2 proposal configuration mode. To remove the encryption algorithm, use the **no** form of this command.

encryption { **des** | **3des** | **aes-cbc-128** | **aes-cbc-192** | **aes-cbc-256** }
no encryption

Syntax Description

des	Specifies 56-bit Data Encryption Standard (DES)-CBC as the encryption algorithm.
3des	Specifies 168-bit DES (3DES) as the encryption algorithm.
aes-cbc-128	Specifies 128-bit Advanced Encryption Standard (AES) as the encryption algorithim.
aes-cbc-192	Specifies 192-bit AES as the encryption algorithim.
aes-cbc-256	Specifies 256-bit AES as the encryption algorithim.

Command Default

The encryption algorithm is not specified.

Command Modes

IKEv2 proposal configuration (config-ikev2-proposal)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE encryption (IKEv2 proposal) command.

Examples

The following example configures an IKE proposal with the aes-cbc-128 and aes-cbc-256 encryption algorithm (all other parameters are set to the defaults):

```
crypto ikev2 proposal p1-global
encryption aes-cbc-128 aes-cbc-256
```

enrollment selfsigned

To specify self-signed enrollment for a trustpoint, use the **enrollment self** command in ca-trustpoint configuration mode. To delete self-signed enrollment from a trustpoint, use the **no** form of this command.

enrollment self
no enrollment self

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default behavior or values.

Command Modes

ca-trustpoint configuration (ca-trustpoint)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE enrollment selfsigned command.

Examples

The following example shows a self-signed certificate being designated for a trustpoint named local:

```
crypto pki trustpoint local
 enrollment self
```

group (IKEv2 proposal)

To specify one or more Diffie-Hellman (DH) group identifier(s) for use in an Internet Key Exchange Version 2 (IKEv2) proposal, use the **group**command in IKEv2 proposal configuration mode. To reset the DH group identifier to the default value, use the **no** form of this command.

group *group type*
no group

Syntax Description

group type	Specifies the DH group.

Command Default

DH group 2 and 5 in the IKEv2 proposal.

Command Modes

IKEv2 proposal configuration (config-ikev2-proposal)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE group (IKEv2 proposal command.

Examples

The following example shows how to configure an IKEv2 proposal with the 2048-bit, 3072-bit, 4096-bit, and 1024-bit DH group:

```
Device(config)#  crypto ikev2 proposal p1-global
Device(config-ikev2-proposal)# group 1 2 5 14 15 16 19 20 21 24
```

integrity

To specify one or more integrity algorithms for an Internet Key Exchange Version 2 (IKEv2) proposal, use the **integrity** command in IKEv2 proposal configuration mode. To remove the configuration of the hash algorithm, use the **no** form of this command.

integrity *integrity type*
no integrity

Syntax Description

integrity type	Specifies the hash algorithm.

Command Default

The default integrity algorithm is used.

Command Modes

IKEv2 proposal configuration (config-ikev2-proposal)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE integrity command.

Examples

The following example configures an IKEv2 proposal with the sha1, sha256, sha384, and sha512 integrity algorithms:

```
Device(config)#  crypto ikev2 proposal p1-global
Device(config-ikev2-proposal)# integrity md5 sha1 sha256 sha384 sha512
```

keyring (IKEv2 profile)

To specify a locally defined or accounting, authentication and authorization (AAA)-based keyring, use the **keyring** command in IKEv2 profile configuration mode. To delete the keyring, use the **no** form of this command.

keyring { **local** *keyring-name* | **aaa** *list-name* [**name-mangler** *mangler-name* | **password** *password*] }
no keyring

Syntax Description

local	Specifies the local keyring.
keyring-name	The keyring name for a locally defined keyring.
aaa	Specifies the AAA-based preshared keys list name.
list-name	The AAA method list name.
name-mangler	Derives the username from the peer identity in the preshared key lookup on the AAA list.
mangler-name	(Optional) Globally defined name mangler.
password *password*	Specifies a password for the password. This argument defines the following values: • **0**—Specifies that the password is unencrypted. • **6**—Specifies that the password is encrypted. • *password*—Specifies an unencrypted user password.

Command Default

A keyring is not specified.

Command Modes

IKEv2 profile configuration (crypto-ikev2-profile)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE keyring (IKEv2 profile) command.

Examples

The following example shows how to configure a locally defined keyring:

```
Router(config)# crypto ikev2 profile if-ipsec256-ikev2-profile
Router(config-ikev2-profile)# keyring local if-ipsec256-ikev2-keyring
```

lifetime (IKEv2 profile)

To specify the lifetime for an Internet Key Exchange Version 2 (IKEv2) security association (SA), use the **lifetime** command in IKEv2 profile configuration mode . To reset the SA lifetime to the default value, use the **no** form of this command.

lifetime *seconds*
no lifetime

Syntax Description

seconds	The time that each IKE SA should exist before expiring. Use an integer from 60 to 86,400 seconds.

Command Default

The default is 86,400 seconds (one day).

Command Modes

IKEv2 profile configuration (config-ikev2-profile)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE lifetime (IKEv2 profile) command

Examples

The following example configures an IKEv2 profile with a security association lifetime of 86400 seconds, and all other parameters are set to the defaults:

```
Router(config)# crypto ikev2 profile if-ipsec256-ikev2-profile
Router(config-ikev2-profile)# lifetime 86400
```

match identity remote

To define the remote identity match statement, use the **match identity remote** command in IKEv2-profile configuration mode. To remove the remote identity match statement, use the **no** form of this command.

match identity remote { **address** *ipv4-address* | **any** | **email** { *email-address* | **domain** *domain-name* } | **fqdn** { **domain** *domain-name domain-name* } | **key-id** *opaque-string* }
no match identity remote { **address** *ipv4-address* | **any** | **email** { *email-address* | **domain** *domain-name* } | **fqdn** { **domain** *domain-name domain-name* } | **key-id** *opaque-string* }

Syntax Description

address *ipv4-address*	Matches peer identity based on remote IPv4 address.
any	Matches any peer identity.
email *email-address*	Matches peer identity based on email address.
domain *domain-name*	Specifies to match peer identity based on domain.
fqdn	Matches peer identity based on FQDN.
domain-string	Specifies the domain string to match.
key-id *opaque-string*	Matches peer identity based on remote key ID.

Command Default

No default behavior or values.

Command Modes

IKEv2 profile configuration (config-ikev2-profile)#

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command is qualified for use in Cisco vManage CLI templates.

Usage Guidelines

An IKEv2 profile is a repository of the nonnegotiable parameters of the IKE security association, such as local or remote identities and authentication methods and the services that are available to the authenticated peers that match the profile. An IKEv2 profile must be attached to either a crypto map or an IPSec profile on both IKEv2 initiator and IKEv2 responder. During IKE AUTH Internet Security Association and Key Management Protocol (ISAKMP) negotiations, the peers must identify themselves to each other.

An IKEv2 profile must contain a match identity or a match certificate statement. An IKEv2 profile can have more than one match identity or match certificate statements.

This command can be used to define the remote identity match statement.

Examples

The following example shows how to define the IKEv2 profile if-ipsec256-ikev2-profile to match the peer identity based on IPv4 address:

```
Device(config)# crypto ikev2 profile if-ipsec256-ikev2-profile
Device(config-ikev2-profile)# match identity remote address 172.16.93.2
```

The following example shows how to define the IKEv2 profile if-ipsec256-ikev2-profile to match any peer identity:

```
Device(config)# crypto ikev2 profile if-ipsec256-ikev2-profile
Device(config-ikev2-profile)# match identity remote any
```

The following example shows how to define the IKEv2 profile if-ipsec256-ikev2-profile to match the peer identity based on FQDN. To match the entire domain, use the domain keyword:

```
Device(config)# crypto ikev2 profile if-ipsec256-ikev2-profile
Device(config-ikev2-profile)# match identity remote fqdn remote.cisco.com
Device(config-ikev2-profile)# match identity remote fqdn domain cisco.com
```

The following example shows how to define the IKEv2 profile if-ipsec256-ikev2-profile to match the peer identity based on email. To match the entire domain, use the domain keyword:

```
Device(config)# crypto ikev2 profile if-ipsec256-ikev2-profile
Device(config-ikev2-profile)# match identity remote email remote@cisco.com
Device(config-ikev2-profile)# match identity remote email domain cisco.com
```

The following example shows how to define the IKEv2 profile if-ipsec256-ikev2-profile to match the peer identity based on key-ID:

```
Device(config)# crypto ikev2 profile if-ipsec256-ikev2-profile
Device(config-ikev2-profile)# match identity remote key-id cisco
```

mode (IPSec)

To change the mode for a transform set, use the **mode** command in crypto transform configuration mode. To reset the mode to the default value of tunnel mode, use the **no** form of this command.

mode { **tunnel** | **transport** }
no mode

Syntax Description

tunnel | **transport**	Specifies the mode for a transform set: either tunnel or transport mode. If neither **tunnel** nor **transport** is specified, the default (tunnel mode) is assigned.

Command Default

Tunnel mode

Command Modes

Crypto transform configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE mode (IPSec) command.

Examples

The following example defines a transform set and changes the mode to transport mode. The mode value only applies to IP traffic with the source and destination addresses at the local and remote IPSec peers.

```
crypto ipsec transform-set if-ipsec256-ikev2-transform esp-gcm 256
mode transport
exit
```

multi-tenancy

To enable multi-tenancy as a global parameter map, use the **multi-tenancy** command in parameter-map type inspect configuration mode. To disable multi-tenancy as a global parameter map, use the **no** form of this command.

multi-tenancy
no multi-tenancy

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Parameter-map type inspect configuration (config-profile).

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

A parameter map allows you to specify parameters that control the behavior of actions and match criteria sthat are specified under a policy map and a class map respectively, for zone-based firewall policies.

Examples

The following example shows how to enable multi-tenancy as a global parameter map:

```
Device(config)# parameter-map type inspect-global
Device(config-profile)# multi-tenancy
```

parameter-map type inspect-global

To configure a global parameter map and enter parameter-map type inspect configuration mode, use the **parameter-map type inspect-global** command in global configuration mode. To delete a global parameter map, use the **no** form of this command.

parameter-map type inspect-global
no parameter-map type inspect-global

Syntax Description

This comand has no keywords or arguments.

Command Default

Global parameter maps are not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

After you enter the **parameter-map type inspect-global** command, you can enter the commands listed in the table below in parameter-map type inspect-global configuration modes.

Command	Description
aggressive-aging	Enables aggressive aging of half-opened firewall sessions.
alert on	Enables Cisco IOS stateful packet inspection alert messages.
inspect	Enables and disables audit trail messages.
log {**dropped-packets** | **flow-export**}	Logs the dropped packets.
max-incomplete {**low** | **high**} *number-of-connections*	Defines the number of existing half-open sessions that will cause the software to start and stop deleting half-open sessions.
multi-tenancy	Enables Cisco vManage for multitenancy.
vpn zone security	Inspects traffic exchange between multiple service VPNs.

Ensure that you configure the **parameter-map type inspect-global** command with **vpn zone security** command to enable zone-based firewall.

For more information on usage guidelines, see the Cisco IOS XE parameter-map type inspect-global command.

Examples

The following example shows a sample parameter-map type inspect-global configuration:

```
Device(config)# parameter-map type inspect-global
Device(config)# alert on
Device(config-profile)# log dropped-packets
Device(config-profile)# multi-tenancy
Device(config-profile)# vpn zone security allow dia
```

peer

To define the peer or peer group and enter the IKEv2 keyring peer configuration mode, use the **peer** command in IKEv2 keyring configuration mode. To remove the peer or peer group, use the **no** form of this command.

peer *name*
no peer *name*

Syntax Description

name	Defines the name of the peer or peer group.

Command Default

No default behavior or values.

Command Modes

IKEv2 keyring configuration (config-ikev2-keyring)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command is qualified for use in Cisco vManage CLI templates.

Usage Guidelines

IKEv2 supports crypto map-and tunnel protection-based crypto interfaces. An IKEv2 keyring is a repository of symmetric and asymmetric preshared keys and is independent of the IKEv1 keyring. The IKEv2 keyring is associated with an IKEv2 profile and hence, caters to a set of peers that match the IKEv2 profile. IKEv2 keyring keys must be configured in the peer configuration submode that defines a peer subblock. An IKEv2 keyring can have multiple peer subblocks. A peer subblock contains a single symmetric or asymmetric key pair for a peer or peer group identified by any combination of hostname, identity, and IP address. This command can be used to set the name of the peer or peer group.

Examples

The following example shows setting the peer name to if-ipsec256-ikev2-keyring-peer and entering the IKEv2 keyring peer configuration mode:

```
Device(config)# crypto ikev2 keyring if-ipsec256-ikev2-keyring
Device(config-ikev2-keyring)# peer if-ipsec256-ikev2-keyring-peer
Device(config-ikev2-keyring-peer)#
```

Related Commands

Command	Description
address	Specifies an IPv4 or IPv6 address or range for the peer.
description	Specifies the description for the peer.
hostname	Specifies the peer using a hostname.
identity	Identifies the IKEv2 peer.ßß:
pre-shared-key	Specifies the preshared key for the peer.

pre-shared-key

To define the preshared key, use the **pre-shared-key** command in IKEv2 keyring peer configuration mode. To remove the preshared key, use the **no** form of this command.

pre-shared-key *key*
no pre-shared-key

Syntax Description

key	Defines the pre-shared key.

Command Default

By default, the preshared key is symmetric.

Command Modes

IKEv2 keyring peer configuration (config-ikev2-keyring-peer).

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

IKEv2 supports crypto map-and tunnel protection-based crypto interfaces. An IKEv2 keyring is a repository of symmetric and asymmetric preshared keys and is independent of the IKEv1 keyring. The IKEv2 keyring is associated with an IKEv2 profile and hence, caters to a set of peers that match the IKEv2 profile. IKEv2 keyring keys must be configured in the peer configuration submode that defines a peer subblock. An IKEv2 keyring can have multiple peer subblocks. A peer subblock contains a single symmetric or asymmetric key pair for a peer or peer group identified by any combination of hostname, identity, and IP address. Use the **pre-shared-key** command to specify the preshared key for the peer.

Examples

The following example shows setting the IKEv2 Keyring with Asymmetric Preshared Keys. The local preshared key is encrypted and named key1. The remote preshared key is unencrypted and named key2:

```
Device(config)# crypto ikev2 keyring if-ipsec256-ikev2-keyring
Device(config-ikev2-keyring)# peer if-ipsec256-ikev2-keyring-peer
Device(config-ikev2-keyring-peer)# hostname if-ipsec256-ikev2-keyring-peer
Device(config-ikev2-keyring-peer)# address 10.0.0.1 255.255.255.0
Device(config-ikev2-keyring-peer)# identity address 10.0.0.5
Device(config-ikev2-keyring-peer)# pre-shared-key cisco123
```

Table 15: Related Commands

Command	Description
address	Specifies an IPv4 or an IPv6 address or range for the peer.
description	Specifies the description for the peer.

Command	Description
hostname	Specifies the peer using a hostname.
identity	Identifies the IKEv2 peer.

proposal

To attach a proposal to an IKEv2 policy, use the **proposal** command in IKEv2 policy configuration mode. To remove a proposal from an IKEv2 policy, use the **no** form of this command.

proposal *name*
no proposal *name*

Syntax Description

name	Specifies the name of the proposal in an IKEv2 policy

Command Default

No default behavior or values.

Command Modes

IKEv2 policy configuration (config-ikev2-policy)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command is qualified for use in Cisco vManage CLI templates.

Usage Guidelines

An IKEv2 policy contains proposals that are used to negotiate the encryption, integrity, PRF algorithms, and DH group in SA_INIT exchange. It can have match statements which are used as selection criteria to select a policy during negotiation. An IKEv2 proposal is a collection of transforms used in the negotiation of IKE security associations as part of the IKE_SA_INIT exchange. Each profile can have multiple proposals and are prioritized in the order of listing. The default proposal is used if no proposals have been attached. This command can be used to attach a proposal to an IKEv2 policy.

Examples

The following example shows how to create the proposal p1-global and attach it to the IKEv2 policy policy1-global:

```
Device(config)# crypto ikev2 proposal p1-global
Device(config-ikev2-proposal)# encryption aes-cbc-128
Device(config-ikev2-proposal)# integrity md5
Device(config-ikev2-proposal)# exit
Device(config)# crypto ikev2 policy policy1-global
Device(config-ikev2-policy)# proposal p1-global
```

revocation-check

To check the revocation status of a certificate, use the **revocation-check crl** command in ca-trustpoint configuration mode. To disable this functionality, use the **revocation-check none** command.

revocation-check crl
revocation-check none

Syntax Description

none	Certificate checking is disabled.

Command Default

After a trustpoint is enabled, the default is set to **revocation-check crl**, which means that CRL checking is mandatory.

Command Modes

Ca-trustpoint configuration (ca-trustpoint)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE revocation check command.

Examples

The following example shows how revocation check is ignored:

```
Device(config)# crypto pki trustpoint TP-self-signed-3865005142
Device(ca-trustpoint)# revocation-check none
```

set ikev2-profile

To attach an IKEv2 profile to an IPSec profile, use the **set ikev2-profile** command in IPSec profile configuration mode. To remove the IKEv2 profile from an IPSec profile, use the no form of this command.

set ikev2-profile *profile-name*
no set ikev2-profile

Syntax Description

profile-name	Specifies the IKEv2 profile name

Command Default

No default behavior or values.

Command Modes

IPSec profile configuration (ipsec-profile)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command is qualified for use in Cisco vManage CLI templates.

Usage Guidelines

An IKEv2 profile is a repository of the nonnegotiable parameters of the IKE security association, such as local or remote identities and authentication methods and the services that are available to the authenticated peers that match the profile. An IKEv2 profile must be attached to either crypto map or IPSec profile on both IKEv2 initiator and responder. An IPSec profile defines the IPsec parameters that are to be used for IPsec encryption between two IPsec devices. This command can be used to attach an IKEv2 profile to an IPSec profile.

Examples

The following example shows how to create the prerequisites — IKEv2 keyring, PKI Trustpoint, IKEv2 profile and how to attach the IKEv2 profile to the IPSec profile if-ipsec256-ipsec-profile:

```
Device(config)# crypto ikev2 keyring if-ipsec256-ikev2-keyring
Device(config-ikev2-keyring)# peer if-ipsec256-ikev2-keyring-peer
Device(config-ikev2-keyring-peer)# hostname if-ipsec256-ikev2-keyring-peer
Device(config-ikev2-keyring-peer)# address 10.0.0.1 255.255.255.0
Device(config-ikev2-keyring-peer)# identity address 10.0.0.5
Device(config-ikev2-keyring-peer)# pre-shared-key cisco123
Device(config-ikev2-keyring-peer)# exit
Device(config-ikev2-keyring)# exit

Device(config)# crypto ikev2 profile if-ipsec256-ikev2-profile
Device(config-ikev2-profile)# authentication local ecdsa-sig
Device(config-ikev2-profile)# aaa authorization group cert list list1
Device(config-ikev2-profile)# keyring local if-ipsec256-ikev2-keyring
Device(config-ikev2-profile)# lifetime 86400
Device(config-ikev2-profile)# match address local 10.10.10.10
Device(config-ikev2-profile)# exit

Device(config)# crypto ipsec profile if-ipsec256-ipsec-profile
Device(ipsec-profile)# set ikev2-profile if-ipsec256-ikev2-profile
```

Related Commands

Command	Description
setidentity	Specifies which identity can be used
setisakmp-profile	Specifies which isakmp-profile can be used
setmixed-mode	Specifies which mixed-mode can be used
setpfs	Specifies which pfs can be used
setreverse-route	Specifies which reverse-route can be used
setsecurity-association	Specifies which security-association can be used
setsecurity-policy	Specifies which security-policy can be used
settransform-set	Specifies which transform sets can be used

set pfs

To optionally specify that IP security (IPsec) requests the perfect forward secrecy (PFS) Diffie-Hellman (DH) prime modulus group identifier when requesting new security associations (SAs) for a crypto map entry or

when IPsec requires PFS when receiving requests for new SAs, use the **set pfs** command in crypto m ap configuration mode. To specify that IPsec should not request PFS during the DH exchange, use the **no** form of this command.

set pfs [group1 | group2 | group5 | group14 | group15 | group16 | group19 | group20 | group21 | group24]
no set pfs

Syntax Description

group1	Specifies the 768-bit DH identifier.
group2	Specifies the 1024-bit DH identifier.
group5	Specifies the 1536-bit DH identifier.
group14	Specifies the 2048-bit DH identifier.
group15	Specifies the 3072-bit DH identifier.
group16	Specifies the 4096-bit DH identifier.
group19	Specifies the 256-bit elliptic curve DH (ECDH) identifier.
group20	Specifies the 384-bit ECDH identifier.
group21	Specifies the 521-bit DH identifier.
group24	Specifies the 2048-bit DH identifier.

Command Default

By default, PFS is not requested. If no group is specified with this command, the **group1** keyword is used as the default.

Command Modes

Crypto map configuration (config-crypto-map)

IPsec profile configuration (ipsec-profile)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE set pfs command.

Examples

The following example specifies that PFS should be used whenever a new security association is negotiated for the crypto ipsec profile if-ipsec256-ipsec-profile:

```
 crypto ipsec profile if-ipsec256-ipsec-profile
 set ikev2-profile if-ipsec256-ikev2-profile
set pfs group16
```

set security-association lifetime

To set the TEK lifetime for a specific crypto map entry or IPsec profile that is used when negotiating IPsec security associations (SAs), use the **set security-association lifetime** command in crypto map configuration mode or IPsec profile configuration mode. To reset a lifetime to the global value, use the **no** form of this command.

set security-association lifetime {**days** *number-of-days* | **kilobytes** {*number-of-kilobytes* | **disable**} | **seconds** *number-of-seconds*}
no set security-association lifetime { **days** | **seconds** }

Syntax Description

days *number-of-days*	Lifetime in days. The range is 1 to 30.
kilobytes *number-of-kilobytes*	Volume of traffic (in kilobytes) that can pass between IPsec peers using an SA. The range is 2560 to 4294967295.
disable	Disables the SA rekey based on the traffic-volume lifetime.
seconds *number-of-seconds*	Lifetime in seconds. The range is 120 to 2592000. **Note** It is not recommended to use a lifetime value that is lower than 900 seconds in production routers.

Command Default

Global lifetime values are used.

Command Modes

IPsec profile configuration (ipsec-profile)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE set security-association lifetime command.

Examples

The following example shows how to disable the SA rekey based on the traffic-volume lifetime for an IPsec profile named if-ipsec256-ipsec-profile:

```
Device# configure-t
Device(config)#  crypto ipsec profile if-ipsec256-ipsec-profile
Device(ipsec-profile)# set ikev2-profile if-ipsec256-ikev2-profile
Device(ipsec-profile)# set pfs group16
Device(ipsec-profile)# set transform-set if-ipsec256-ikev2-transform
Device(ipsec-profile)# set security-association lifetime kilobytes disable
```

set security-association replay window-size

To control the security associations (SAs) that are created using the policy specified by a particular crypto map, dynamic crypto map, or crypto profile, use the **set security-association replay window-size**command in crypto map configuration or crypto profile configuration mode. To reset the crypto map to follow the global configuration that was specified by the **crypto ipsec security-association replay window-size** command, use the **no** form of this command.

set security-association replay window-size [*N*]
no set security-association replay

Syntax Description

N	(Optional) Size of the window. The value can be 64, 128, 256, 512, or 1024. This value sets the window size for a particular crypto map, dynamic crypto map, or crypto profile.

Command Default

Window size is not set.

Command Modes

Crypto map configuration
Crypto profile configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Examples

The following example shows that the window size has been set to 512 for the crypto ispec profile named "if-ipsec256-ipsec-profile":

```
crypto ipsec profile if-ipsec256-ipsec-profile
set ikev2-profile if-ipsec256-ikev2-profile
set pfs group16
set transform-set if-ipsec256-ikev2-transform
set security-association lifetime seconds 3600
set security-association replay window-size 512
```

set transform-set

To specify which transform sets can be used with the crypto map entry, use the **set transform-set**command in crypto map configuration mode. To remove all transform sets from a crypto map entry, use the **no** form of this command.

set transform-set *transform-set-name*
[*transform-set2...transform-set6*]
no set transform-set

Syntax Description

transform-set-name	Name of the transform set. For an **ipsec-manual** crypto map entry, you can specify only one transform set. For an **ipsec-isakmp** or dynamic crypto map entry, you can specify up to six transform sets.

Command Default

No transform sets are included by default.

Command Modes

IPsec profile configuration (ipsec-profile)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE set transform-set command.

Examples

The following example defines a transform set and specifies that it can be used with a crypto ispec profile.

```
 crypto ipsec transform-set if-ipsec256-ikev2-transform esp-gcm 256
mode tunnel
!
crypto ipsec profile if-ipsec256-ipsec-profilep
set ikev2-profile if-ipsec256-ikev2-profile
set pfs group16
set transform-set if-ipsec256-ikev2-transform
```

subject-name

To specify the subject name in the certificate request, use the **subject-name** command in ca-trustpoint configuration mode. To clear any subject name from the configuration, use the **no** form of this command.

subject-name *name*
no subject-name *name*

Syntax Description

name	Specifies the subject name used in the certificate request.

Command Default

If the *name* argument is not specified, the fully qualified domain name (FQDN), which is the default subject name, will be used.

Command Modes

Ca-trustpoint configuration (ca-trustpoint)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

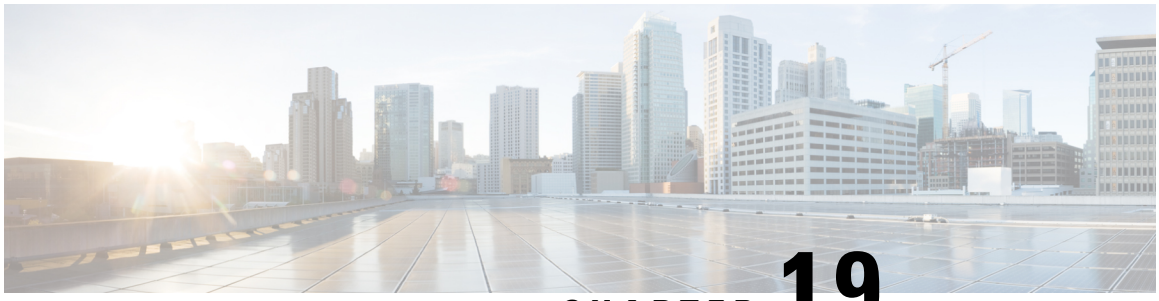
Usage Guidelines

For usage guidelines, see the Cisco IOS XE subject-name command.

Examples

The following example shows how to specify the subject name for the certificate:

```
crypto pki trustpoint TP-self-signed-3865005142
  enrollment selfsigned
  revocation-check none
  subject-name     cn=IOS-Self-Signed-Certificate-3865005142
```



CHAPTER 19

EIGRP Commands

- address-family ipv4 vrf autonomous-system, on page 227
- af-interface, on page 228
- dampening-change, on page 229
- dampening-interval, on page 230
- exit-address-family, on page 230
- exit-af-interface, on page 231
- exit-af-topology, on page 232
- hello-interval, on page 233
- hold-time, on page 233
- neighbor (EIGRP), on page 234
- network (EIGRP), on page 235
- redistribute omp metric , on page 236
- redistribute static , on page 237
- router eigrp, on page 237
- split-horizon (EIGRP), on page 238
- topology (EIGRP), on page 239

address-family ipv4 vrf autonomous-system

To enter router address family configuration mode to configure the Enhanced Interior Gateway Routing Protocol (EIGRP) for Multitopology Routing (MTR), use the **address-family ipv4 vrf autonomous-system** command in router configuration mode. To remove the address family from the EIGRP configuration, use the **no** form of this command.

address-family ipv4 vrf *vrf-number*[**unicast** | **multicast**] **autonomous-system** *as-number*
no address-family ipv4 vrf *vrf-number*[**unicast** | **multicast**] **autonomous-system** *as-number*

Syntax Description

unicast	(Optional) Specifies the unicast subaddress family.
multicast	(Optional) Specifies the multicast subaddress family.
vrf *vrf-number*	Specifies the number for VRF.
autonomous-system *as-number*	Specifies the autonomous system number.

Command Default This command is disabled by default.

Command Modes Router configuration (config-router)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines The **address-family ipv4 vrf autonomous-system** command is used to enter router address family or subaddress family configuration mode to configure the exchange of address-family and subaddress-family prefixes.

For usage guidelines, see the Cisco IOS XE `address-family ipv4` command.

Examples The following example shows how to configure an IPv4 address family to associate with the MTR topology named base:

```
Device(config)# router eigrp mtr
Device(config-router)# address-family ipv4 vrf 1 autonomous-system 5 topology base
```

af-interface

To enter address-family interface configuration mode and to configure interface-specific Enhanced Interior Gateway Routing Protocol (EIGRP) commands, use the **af-interface** command in address-family configuration mode. To reset the address-family interface setting to factory values, use the **no** form of this command.

af-interface { **default** | *interface-type* *interface-number* }
no af-interface

{ **default** | *interface-type* *interface -number* }

Syntax Description

default	Specifies the default address-family interface configuration mode. Commands applied under this mode affect all interfaces used by this address-family instance.
interface-type interface-number	Interface type and number of the interface that the address-family submode commands will affect.

Command Default Address-family interface configuration mode is not entered.

Command Modes Address-family configuration (config-router-af)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `af-interface` command.

Examples

The following example shows how to enter address-family interface configuration mode and to configure EIGRP interface-specific commands:

```
Device(config)# router eigrp virtual-name
Device(config-router)# address-family ipv4 vrf 1 autonomous-system 5
Device(config-router-af)# af-interface interface-name
```

dampening-change

To set a threshold percentage to minimize or dampen the effect of frequent routing changes through an interface in an Enhanced Interior Gateway Routing Protocol (EIGRP) address family or service family, use the **dampening-change** command in address-family interface configuration mode or service-family interface configuration mode. To restore the default value, use the **no** form of this command.

dampening-change [*change-percentage*]
no dampening-change

Syntax Description

change-percentage	(Optional) The percentage a metric must change before the value is stored for future decisions on advertisements. Value range is 1 to 100. If a *change-percentage* value is not specified, the default is 50 percent of the computed metric.

Command Default

No threshold percentage is configured.

Command Modes

Address-family interface configuration (config-router-af-interface) Service-family interface configuration (config-router-sf-interface)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `dampening-change` command.

Examples

The following example configures an EIGRP address family to accept a peer metric change if the change is greater than 75 percent of the last updated value:

```
Device(config)# router eigrp virtual-name
Device(config-router)# address-family ipv4 vrf 1 autonomous-system 5400
Device(config-router-af)# af-interface ethernet0/0
Device(config-router-af-interface)# dampening-change 75
```

dampening-interval

To set a threshold time interval to minimize or dampen the effect of frequent routing changes through an interface in an Enhanced Interior Gateway Routing Protocol (EIGRP) address family or service family, use the **dampening-interval** command in address-family interface configuration mode or service-family interface configuration mode. To restore to the default value, use the **no** form of this command.

dampening-interval [*interval*]
no dampening-interval [*interval*]

Syntax Description

interval	(Optional) Time interval, in seconds, that must elapse before a route change will cause an update to occur. Value range is 1 to 65535. If an *interval* value is not specified, the default is 30 seconds.

Command Default

A dampening interval is not enabled.

Command Modes

Address-family interface configuration (config-router-af-interface) Service-family interface configuration (config-router-sf-interface)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `dampening-interval` command.

Examples

The following example configures EIGRP address-family Ethernet interface 0/0 to limit the metric change frequency to no more than one change in a 45-second interval:

```
Device(config)# router eigrp virtual-name

Device(config-router)# address-family ipv4 vrf 1 autonomous-system 5400
Device(config-router-af)# af-interface ethernet0/0
Device(config-router-af-interface)# dampening-interval 45
```

exit-address-family

To exit from address-family configuration mode, use the **exit-address-family** command in address-family configuration mode.

exit-address-family

Syntax Description

This command has no arguments or keywords.

Command Default

The router remains in address-family configuration mode.

Command Modes

Address-family configuration (config-router-af) VRF address-family configuration (config-vrf-af)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

Use the **exit-address-family** command to exit address-family configuration mode and return to router configuration mode.

This command can be abbreviated to **exit**.

For usage guidelines, see the Cisco IOS XE `exit-address-family` command.

Examples

The following example shows how to exit address-family configuration mode and return to router configuration mode:

```
Device(config)# router eigrp virtual-name
Device(config-router)# address-family ipv4 vrf 1 autonomous-system 4453

Device(config-router-af)# exit-address-family

Device(config-router)#
```

The following example shows how to exit VRF address-family configuration mode and return to VRF configuration mode:

```
Device(config)# vrf definition vrf1
Device(config-vrf)# address-family ipv6
Device(config-vrf-af)# exit-address-family

Device(config-vrf)#
```

exit-af-interface

To exit address-family interface configuration mode, use the **exit-af-interface** command in address-family interface configuration mode.

exit-af-interface

Syntax Description

This command has no arguments or keywords.

Command Default

The router remains in address-family interface configuration mode.

Command Modes

Address-family interface configuration (config-router-af-interface)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

Use the **exit-af-interface** command to exit address-family interface configuration mode and return to address-family configuration mode.

For usage guidelines, see the Cisco IOS XE `exit-af-interface` command.

Examples

The following example shows how to exit address-family interface configuration mode:

```
Device(config)# router eigrp virtual-name
Device(config-router)# address-family ipv4 vrf 1 autonomous-system 4453
Device(config-router-af)# af-interface af-interface-name
Device(config-router-af-interface)# exit-af-interface
Device(config-router-af)#
```

exit-af-topology

To exit address-family topology configuration mode, use the **exit-af-topology** command in address-family topology configuration mode.

exit-af-topology

Syntax Description

This command has no arguments or keywords.

Command Default

The router remains in address-family topology configuration mode.

Command Modes

Address-family topology configuration (config-router-af-topology)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

Use the **exit-af-topology** command to exit address-family topology configuration mode and return to address-family configuration mode.

For usage guidelines, see the Cisco IOS XE `exit-af-topology` command.

Examples

The following example shows how to exit address-family topology configuration mode:

```
Device(config)# router eigrp virtual-name
Device(config-router)# address-family ipv4 vrf 1 autonomous-system 4453
Device(config-router-af)# topology base
Device(config-router-af-topology)# exit-af-topology
Device(config-router-af)#
```

hello-interval

To configure the hello interval for the Enhanced Interior Gateway Routing Protocol (EIGRP) address-family configuration, use the **hello-interval** command in address-family interface configuration mode. To configure the default hello interval, use the **no** form of this command.

hello-interval *seconds*
no hello-interval

Syntax Description

seconds	Hello interval in seconds. The range is 1 to 65535. The default is 60 for low-speed nonbroadcast multiaccess (NBMA) networks, and 5 for all other networks.

Command Default

The EIGRP hello interval is 60 seconds for low-speed NBMA networks and 5 seconds for all other networks.

Command Modes

Address-family interface configuration (config-router-af-interface)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `hello-interval` command.

Examples

The following example configures a 10-second hello interval for address-family Ethernet interface 0/0:

```
Device(config)# router eigrp virtual-name
Device(config-router)# address-family ipv4 vrf 1 autonomous-system 4453
Device(config-router-af-interface)# af-interface ethernet0/0
Device(config-router-af-interface)# hello-interval 10
```

hold-time

To configure the hold time for Enhanced Interior Gateway Routing Protocol (EIGRP) address-family, use the **hold-time** command in address-family interface configuration mode. To configure the default hold time, use the **no** form of this command.

hold-time *seconds*
no hold-time

Syntax Description

seconds	Interval, in seconds, before a neighbor is considered down. Valid range is 1 to 65535 seconds (approximately 18 hours). The default is 180 seconds for low-speed nonbroadcast multiaccess (NBMA) networks and 15 seconds for all other networks.

Command Default

The EIGRP hold time is 180 seconds for NBMA networks and 15 seconds for all other networks.

Command Modes Address-family interface configuration (config-router-af-interface)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines On very congested and large networks, the default hold time may not be sufficient for all routers and access servers to receive hello packets from neighbors. In this case, increase the hold time duration. The hold time should be at least three times the hello interval. If a router does not receive a hello packet within the specified hold time, services through this router are considered unavailable. Increasing the hold time will delay route convergence across the network.

For usage guidelines, see the Cisco IOS XE `hold-time` command.

Examples The following example sets a 50-second hold time for address-family Ethernet interface 0/0:

```
Device(config)# router eigrp virtual-name
Device(config-router)# address-family ipv4 vrf 1 autonomous-system 4453
Device(config-router-af-interface)# af-interface ethernet0/0
Device(config-router-af-interface)# hold-time 50
```

neighbor (EIGRP)

To define a neighboring device with which an Enhanced Interior Gateway Routing Protocol (EIGRP) device can exchange routing information, use the **neighbor** command in the address family configuration mode. To remove an entry, use the **no** form of this command.

neighbor {*ip-address ipv6-address*} *interface-type interface-number*
no neighbor {*ip-addressipv6-address*} *interface-type interface-number*

Syntax Description

ip-address	IP address of a peer router with which routing information will be exchanged.
ipv6-address	IPv6 address of a peer router with which routing information will be exchanged.
interface-type	Interface or subinterface through which peering sessions are established.
interface-number	Number of the interface or subinterface.

Command Default No neighboring routers are defined.

Command Modes Address family configuration (config-router-af)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

Multiple neighbor statements can be used to establish peering sessions with specific EIGRP neighbors. The interface through which EIGRP exchanges routing updates must be specified in the neighbor statement. The interfaces through which two EIGRP neighbors exchange routing updates must be configured with IP addresses from the same network.

For usage guidelines, see the Cisco IOS XE `neighbor` command.

Examples

The following example shows how to configure EIGRP peering sessions with neighbors 192.168.1.1 and 192.168.2.2:

The following named configuration example shows how to configure EIGRP to send address-family updates to specific neighbors:

```
Device(config)# router eigrp virtual-name
Device(config-router)# address-family ipv4 vrf 1 autonomous-system 4453
Device(config-router-af)# neighbor 192.168.1.10 1
Device(config-router-af)# neighbor 10.1.1.2 loopback 0 remote 10
```

network (EIGRP)

To specify the network for an Enhanced Interior Gateway Routing Protocol (EIGRP) routing process, use the **network** command in address-family configuration mode. To remove an entry, use the **no** form of this command.

network *ip-address* [*wildcard-mask*]
no network *ip-address*

Syntax Description

ip-address	IP address of the directly connected network.
wildcard-mask	(Optional) EIGRP wildcard bits. Wildcard mask indicates a subnetwork, bitwise complement of the subnet mask.

Command Default

No networks are specified.

Command Modes

Address-family configuration (config-router-af)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `network` command.

Examples

The following example configures EIGRP autonomous system 1 and establishes neighbors through network 172.16.0.0 and 192.168.0.0:

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 vrf 1 autonomous-system 4453
Device(config-router-af)# network 172.16.0.0
Device(config-router-af)# network 192.168.0.0
```

redistribute omp metric

To redistribute OMP routes into EIGRP, use the **redistribute omp metric** command in (EIGRP Named Mode) Address-family Topology configuration mode. To disable redistribute OMP routes into EIGRP, use the **no** form of this command.

redistribute omp metric { *bandwidth* | *delay* | *reliability* | *load* | *MTU* }

no redistribute omp metric { *bandwidth* | *delay* | *reliability* | *load* | *MTU* }

Syntax Description

bandwidth	In units of kilobits per second; 10000 for Ethernet <1 .. 4294967295>
delay	In units of tens of microseconds; for Ethernet it is 100 x 10 microseconds = 1 ms <0..4294967295>
reliability	255 for 100 percent reliability <unsignedByte, 0 .. 255>
load	Effective load on the link expressed as a number from 1 to 255 (255 is 100 percent loading) <unsignedByte, 1 .. 255>
MTU	Minimum MTU of the path; usually equals that for the Ethernet interface, which is 1500 bytes <1 .. 65535>

Command Default

None

Command Modes

(EIGRP Named Mode) Address-family topology configuration (config-router-af-topology)

Release	Modification
Cisco IOS XE SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

By default, routes from other routing protocols are not redistributed into EIGRP. It can be useful for EIGRP to learn OMP routes, because OMP learns routes to destinations throughout the overlay network. This command can be used to redistribute omp routes into EIGRP.

Example

The following example shows redistributing omp into a named EIGRP process called INSTANCE1 with the following metrics - bandwidth = 1000000, delay = 100, reliability = 255, load = 1, MTU = 1500.

```
Device(config)# router eigrp INSTANCE1
Device(config-router)# address-family ipv4 unicast vrf 1 autonomous-system 100
Device(config-router-af)# topology base
Device(config-router-af-topology)# redistribute omp metric 1000000 100 255 1 1500
```

redistribute static

To redistribute IPv4 routes to Enhanced Interior Gateway Routing Protocol (EIGRP), use the **redistribute static** command in the address-family topology configuration mode. To disable the configuration, use the **no** form of this command

redistribute static

Syntax Description

static	Indicates static route redistribution in eigrp.

Command Default

Route redistribution is disabled.

Command Modes

Address-family topology configuration (config-router-af-topology)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `redistribute eigrp` command.

Examples

The following example shows the behavior of the **redistribute static** command.

```
Device(config)# router eigrp virtual-name
Device(config-router)# address-family ipv4 vrf 1 autonomous-system 4453
Device(config-router-af)# topology base
Device(config-router-af-topology)# redistribute static
```

router eigrp

To configure the Enhanced Interior Gateway Routing Protocol (EIGRP) routing process, use the **router eigrp** command in global configuration mode. To remove an EIGRP routing process, use the **no** form of this command.

router eigrp *virtual-instance-name*
no router eigrp *virtual-instance-name*

Syntax Description

virtual-instance-name	EIGRP virtual instance name. This name must be unique among all address-family router processes on a single router, but need not be unique among routers.

Command Default

No EIGRP processes are configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `router eigrp` command.

Examples

The following example configures an EIGRP address-family routing process and assigns it the name "virtual-name":

```
Device(config)#
router eigrp virtual-name
```

split-horizon (EIGRP)

To enable Enhanced Interior Gateway Routing Protocol (EIGRP) split-horizon, use the **split-horizon** command in address-family interface configuration mode or service-family interface configuration mode. To disable EIGRP split-horizon, use the **no** form of this command.

split-horizon
no split-horizon

Syntax Description

This command has no arguments or keywords.

Command Default

EIGRP split-horizon is enabled by default. However, for ATM interfaces and subinterfaces **split-horizon** is disabled by default.

Command Modes

Address-family interface configuration (config-router-af-interface) Service-family interface configuration (config-router-sf-interface)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `split-horizon (EIGRP)` command.

Examples

The following example disables EIGRP split-horizon for serial interface 3/0 in address-family 5400:

```
Device(config)# router eigrp virtual-name
Device(config-router)# address-family ipv4 vrf 1 autonomous-system 5400
Device(config-router-af)# af-interface serial3/0
Device(config-router-af-interface)# split-horizon
```

topology (EIGRP)

To configure an Enhanced Interior Gateway Routing Protocol (EIGRP) process to route IP traffic under the specified topology instance and to enter address-family topology configuration mode, use the **topology** command in address-family configuration mode.

topology base
no topology *topology-name*

Syntax Description

base	Specifies the base topology.

Command Default

EIGRP routing processes are not configured to route IP traffic under a topology instance.

Command Modes

Address-family configuration (config-router-af)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

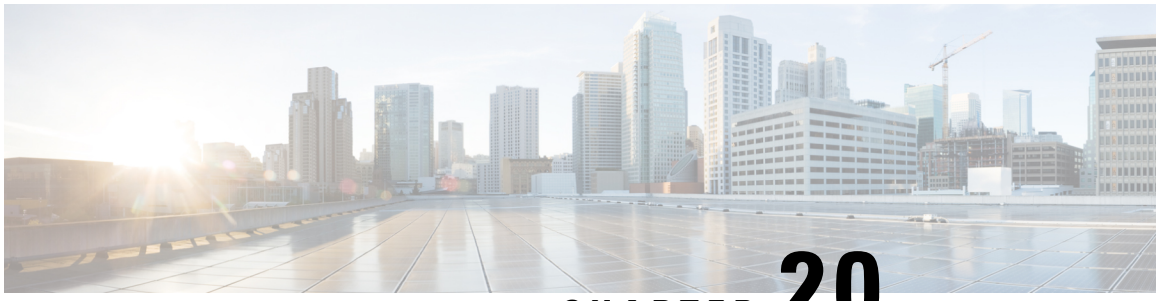
Usage Guidelines

For usage guidelines, see the Cisco IOS XE `topology` command.

Examples

The following example configures EIGRP process 1 to route traffic for the 192.168.0.0/16 network under the VOICE topology instance:

```
Device(config)# router eigrp virtual-name
Device(config-router)# address-family ipv4 vrf 1 autonomous-system 3
Device(config-router-af)# topology base
```



CHAPTER 20

Event Commands

- action (EEM), on page 241
- event ipsla, on page 244
- event manager applet, on page 246
- event manager session cli username, on page 247
- event none, on page 247
- event routing, on page 248
- event syslog, on page 250
- event timer, on page 251
- event track, on page 253

action (EEM)

To match a regular expression pattern on an input string, to specify the action of writing a message to syslog, and to specify the action of reloading the Cisco IOS software when an Embedded Event Manager (EEM) applet is triggered, use the **action** command in applet configuration mode. To disable this function, use the **no** form of this command.

action *label* { **regexp** *string-submatch* | **reload** | **syslog** **msg** *msg-text* | **wait** *wait-interval* | **else** | **break** | **continue** | **elseif** | **while** | **set** | **increment** | **handle-error** | **gets** | **foreach** | **divide** | **decrement** | **counter** | **append** }
no **action** *label*

Syntax Description

label	Unique identifier that can be any string value. Actions are sorted and run in ascending alphanumeric key sequence using the label as the sort key. If the string contains embedded blanks, enclose it in double quotation marks.
string-submatch	(Optional) The variable name to store any submatches that are present. A maximum of three submatch strings can be specified.
msg	Specifies the message to be logged.

msg-text	Character text, an environment variable, or a combination of the two. If the string contains embedded blanks, enclose it in double quotation marks. **Note** Messages written to syslog from an EEM applet are not screened for EEM syslog events, which may lead to recursive EEM syslog events. Messages sent from an EEM applet include the applet name for identification.
wait-interval	The wait interval range is from 1 to 31536000.
else	Identifies the else conditional action block. If a statement is not associated with this applet, events are still triggered without any action or result.
break	Causes an immediate exit from a loop of actions. Skips all the actions down to the related end action.
continue	Causes the loop to continue with the next iteration.
elseif	Identifies the beginning of an elseif conditional action block when an EEM applet is triggered.
while	Identifies the while conditional action block when an EEM applet is triggered.
set	Sets the value of a variable when an EEM applet is triggered.
increment	Increments the value of the variable with the long integer specified.
handle-error	Specifies the error.
gets	Specifies an input from the local tty in a synchronous applet and stores the value in the given variable when an EEM applet is triggered
foreach	Specifies the iteration of an input string using the delimiter as a tokenizing pattern.
divide	Specifies the dividend value by the given divisor value when an EEM applet is triggered.
decrement	Decrements the value of the variable with the integer specified.
counter	Specifies the counter to be set or modified.
append	Appends the given string value to the current value of the variable specified.

Command Default

No messages are written to syslog.

No reload of the Cisco IOS software is performed.

No regular expression patterns are matched.

Command Modes

Applet configuration (config-applet)

Command History

Release	Modifications
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Release	Modifications
Cisco IOS XE Catalyst SD-WAN Release 17.14.1a	The EEM configurations such as else, break, continue, elseif, while, set, increment, handle-error, gets, foreach, divide, decrement, counter, and append are supported.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE action (EEM) commands.

Use the **action else** command to identify the else conditional action block. If a statement is not associated with this applet, events are still triggered without any action or result. A warning message stating that no statements are associated with this applet is displayed at the exit time of the configuration.

Examples

The following example shows how to specify a message to be sent to syslog when the memory-fail applet is triggered:

```
Device(config)# event manager applet memory-fail
```

The following example shows how to reload the Cisco IOS software when the memory-fail applet is triggered:

```
Device(config)# event manager applet memory-fail
Device(config-applet)# action 3.0 reload
```

The following example shows how to define a regular expression match:

```
Device(config-applet)# event manager applet regexp
Device(config-applet)# event none
Device(config-applet)# action 1 regexp "(.*) (.*) (.*)" "one two three" _match _sub1
```

The following example shows how to configure an EEM applet to break from a loop of actions:

```
Device(config)# event manager applet loop
Device(config-applet)# event none
Device(config-applet)# action 1 while 1 eq 1
Device(config-applet)# action 2 break
Device(config-applet)# action 3 end
```

The following example shows how to configure an EEM applet to continue from a loop of actions:

```
Device(config)# event manager applet loop
Device(config-applet)# event none
Device(config-applet)# action 2 continue
Device(config-applet)# action 3 end
```

The following example shows how to identify the beginning of an else action block:

```
Device(config)# event manager applet loop
Device(config-applet)# event none
Device(config-applet)# action label2 else
Device(config-applet)# action 3 end
```

The following example shows how to identify the beginning of the elseif conditional action block.

```
Device(config)# event manager applet action
Device(config-applet)# event none
Device(config-applet)# action 1.0 set x "5"
Device(config-applet)# action 2.0 if $x lt 3
```

```
Device(config-applet)# action 3.0  puts "$x is less than 3"
Device(config-applet)# action 4.0 elseif $x lt 10
Device(config-applet)# action 5.0  puts "$x is less than 10"
Device(config-applet)# action 6.0 end
Device(config)# event manager run action 5 is less than 10
```

event ipsla

To publish an event when an IP SLAs operation is triggered for an Embedded Event Manager (EEM) applet, use the **eventipsla** command in the applet configuration mode. To disable publishing events when an IP SLAs reaction gets triggered, use the **no** form of this command.

event ipsla [**group-name** *name*] [**maxrun** *maxruntime-number*] [**ratelimit** *ratelimit-number*] [**reaction-type** *type*]
no event ipsla

Syntax Description

group-name	Specifies the IP SLAs group ID.
name	Name of the IP SLAs group.
reaction-type	(Optional) Specifies the reaction to be taken for the specified IP SLAs operation.
type	(Optional) Type of IP SLAs reaction. One of the following keywords can be specified: • **connectionLoss**: Specifies that a reaction should occur if there is a one-way connection loss for the monitored operation. • **icpif**: Specifies that a reaction should occur if the one-way Calculated Planning Impairment Factor (ICPIF) value violates the upper threshold or lower threshold. • **jitterAvg**: Specifies that a reaction should occur if the average round-trip jitter value violates the upper threshold or lower threshold. • **jitterDSAvg**: Specifies that a reaction should occur if the average one-way destination-to-source jitter value violates the upper threshold or lower threshold. • **jitterSDAvg**: Specifies that a reaction should occur if the average one-way source-to-destination jitter value violates the upper threshold or lower threshold. • **maxOfNegativeDS**: Specifies that a reaction should occur if the one-way maximum negative jitter destination-to-source threshold is violated. • **maxOfNegativeSD**: Specifies that a reaction should occur if the one-way maximum negative jitter source-to-destination threshold is violated.

	• **maxOfPositiveDS**: Specifies that a reaction should occur if the one-way maximum positive jitter destination-to-source threshold is violated. • **maxOfPositiveSD**: Specifies that a reaction should occur if the one-way maximum positive jitter source-to-destination threshold is violated. • **mos**: Specifies that a reaction should occur if the one-way Mean Opinion Score (MOS) value violates the upper threshold or lower threshold. • **packetLateArrival**: Specifies that a reaction should occur if the one-way number of late packets violates the upper threshold or lower threshold. • **packetLossDS**: Specifies that a reaction should occur if the one-way destination-to-source packet loss value violates the upper threshold or lower threshold. • **packetLossSD**: Specifies that a reaction should occur if the one-way source-to-destination packet loss value violates the upper threshold or lower threshold. • **packetMIA**: Specif ies that a reaction should occur if the one-way number of missing packets violates the upper threshold or lower threshold. • **packetOutOfSequence**: Specifies that a reaction should occur if the one-way number of packets out of sequence violates the upper threshold or lower threshold. • **rtt**: Specifies that a reaction should occur if the round-trip time violates the upper threshold or lower threshold. • **timeout**: Specifies that a reaction should occur if there is a one-way timeout for the monitored operation. • **verifyError**: Specifies that a reaction should occur if there is a one-way error verification violation.
maxrun	(Optional) Specifies the maximum runtime of the applet. If the **maxrun** keyword is specified, the *maxruntime-number* value must be specified. If the **maxrun** keyword is not specified, the default applet run time is 20 seconds.
maxruntime-number	(Optional) Number of seconds specified in *ssssssss* [*mmm*] format, where *ssssssss* must be an integer representing seconds from 0 to 31536000, and where *mmm* must be an integer representing milliseconds from 0 to 999.
ratelimit	(Optional) Specifies the ratelimit time interval of the applet. If the **ratelimit** keyword is specified, the *ratelimit-number* value must be specified.
ratelimit-number	(Optional) Number of seconds specified in *ssssssss* [*mmm*] format, where *ssssssss* must be an integer representing seconds from 0 to 31536000, and where *mmm* must be an integer representing milliseconds from 0 to 999.

Command Default No events are published when IP SLAs operations are triggered.

Command Modes Applet configuration (config-applet)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE event ipsla command.

Examples

The following example shows how to publish an event when an IP SLAs operation is triggered:

```
Device# config-transaction
Device(config)# event manager applet EventIPSLA
Device(config-applet)#  event ipsla group-name grp1 reaction-type timeout maxrun 3
```

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 the command.

event manager applet *applet-name* [**authorization bypass**]
no event manager applet

Syntax Description

applet-name	Name of the applet file.
authorization	(Optional) Specifies AAA authorization type for applet.
bypass	(Optional) Specifies EEM AAA authorization type bypass.

Command Default

No EEM applets are registered.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE event manager applet command.

Examples

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:

```
Device(config)# event manager applet one class A
Device(config-applet)# event timer watchdog time 10
Device(config-applet)# action syslog syslog msg "hello world"
Device(config-applet)# exit
```

The following example shows how to bypass the AAA authorization when registering an applet with the name one and class A.

```
Device(config)# event manager applet one class A authorization bypass
Device(config-applet)#
```

event manager session cli username

To associate a username with Embedded Event Manager (EEM) policies that use the CLI library, use the **event manager session cli username** command in global configuration mode. To remove the username association with EEM policies that use the CLI library, use the **no** form of the command.

event manager session cli username *username* **privilege** *privilege-level*
no event manager session cli

Syntax Description

username	Username assigned to EEM CLI sessions that are initiated by EEM policies.
privilege *privilege-level*	Sets the privilege level for the user. Range: 0 to 15. Default is 1.

Command Modes

Global configuration (config)

Command Default

No username is associated with EEM CLI sessions.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE event manager session cli username command.

Examples

The following example of the **event manager session cli username** command associates the username eemuser with EEM CLI sessions initiated by EEM policies:

```
Device(config)# event manager session cli username eemuser
```

event none

To specify that an Embedded Event Manager (EEM) policy is to be registered with the EEM and can be run manually, use the **event none** command in applet configuration mode. To remove the **event none** command from the configuration file, use the **no** form of the command.

event none [**maxrun** *maxruntime-number*] [**ratelimit** *ratelimit-number*]
no event none

Syntax Description

maxrun	(Optional) Specifies the maximum runtime of the applet. If the **maxrun** keyword is specified, the *maxruntime-number* value must be specified. If the **maxrun** keyword is not specified, the default applet run time is 20 seconds.

maxruntime-number	(Optional) Number of seconds specified in ssssssss.mmm] format, where ssssssss must be an integer representing seconds between 0 and 31536000, inclusive, and where mmm must be an integer representing milliseconds between 0 and 999).
ratelimit	(Optional) Specifies the ratelimit time interval of the applet. If the **ratelimit** keyword is specified, the *ratelimit-number* value must be specified.
ratelimit-number	(Optional) Number of seconds specified in ssssssss [*mmm*] format, where ssssssss must be an integer representing seconds from 0 to 31536000, and where *mmm* must be an integer representing milliseconds from 0 to 999.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE event none command.

Examples

The following example shows how to register a policy named manual-policy to be run manually and then how to execute the policy:

```
Device(config)# event manager applet manual-policy
Device(config-applet)# event none
Device(config-applet)# exit
Device# event manager run manual-policy
```

event routing

To publish an event when route entries change in Routing Information Base (RIB) infrastructure, use the **event routing** command in applet configuration mode. To stop publishing events when route entries change in RIB, use the **no** form of the command.

event routing network *ip-address / length* [**type** { **add** | **all** | **modify** | **remove** }] [**maxrun** *maxruntime-number*] [**ratelimit** *ratelimit-number*]
no event routing

Syntax Description

network	Specifies the network ip address and length, whose route is to be monitored.
ip-address / length	The ip address and length of the network to be monitored. For example, 192.0.2.4/8.
type	(Optional) Specifies the desired policy trigger. The default is **all**.
add	Specifies that an entry is added to the routing table.
all	Specifies that a routing table entry is added, removed, or modified.
modify	Specifies that an entry in the routing table is modified.
remove	Specifies that an entry is removed from the routing table

maxrun	(Optional) Specifies the maximum runtime of the applet. If the **maxrun** keyword is specified, the *maxruntime-number* value must be specified. If the **maxrun** keyword is not specified, the default applet run time is 20 seconds.
maxruntime-number	(Optional) Number of seconds specified in ssssssss[.mmm] format, where ssssssss must be an integer representing seconds from 0 to 31536000, inclusive, and where mmm must be an integer representing milliseconds between 0 and 999.
ratelimit	(Optional) Specifies the ratelimit time interval of the applet. If the **ratelimit** keyword is specified, the *ratelimit-number* value must be specified.
ratelimit-number	(Optional) Number of seconds specified in *ssssssss* [*mmm*] format, where *ssssssss* must be an integer representing seconds from 0 to 31536000, and where *mmm* must be an integer representing milliseconds from 0 to 999.

Command Default

By default, no events are published when route entries change in RIB infrastructure.

Command Modes

Applet configuration (config-applet)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE event routing command.

Examples

The following example shows how a specific route entries change when many parameters are monitored:

```
Device# configure terminal
Device(config)# event manager applet EventRouting
Device(config-applet)# event routing network 192.0.2.4/8 type add maxrun 56
```

The following example shows the output for the Cisco IOS version that uses the old routing API (v1.0):

```
Device# show event manager detector routing
No. Name  Version    Node       Type
1   routing     01.00     node0/0     RP
```

The following example shows the output for the Cisco IOS version that uses the new routing API (v2.0):

```
Device# show event manager detector routing
No. Name  Version    Node       Type
1   routing     02.00     node0/0     RP
```

event syslog

To specify the event criteria for an Embedded Event Manager (EEM) applet that is run by matching syslog messages, use the **event syslog** command in applet configuration mode. To remove the syslog message event criteria, use the **no** form of the command.

event syslog [**pattern** *regular-expression*] [**occurs** *num-occurrences*] [**period** *period-value*] [**ratelimit** *ratelimit-number*] [**maxrun** *maxruntime-number*]
no event syslog

Syntax Description

pattern	Specifies that a regular expression is used to perform the syslog message pattern match.
regular-expression	String value that is the pattern to be matched.
occurs	(Optional) Specifies the number of matching occurrences before an EEM event is triggered. If a number is not specified, an EEM event is triggered after the first match.
num-occurrences	(Optional) Integer in the range of 1 to 32, inclusive.
period	(Optional) Specifies the time interval during which the one or more occurrences must take place. If the **period** keyword is not specified, no time-period check is applied.
period-value	(Optional) Number that represents seconds and optional milliseconds in the format sssssssss[.mmm]. The range for seconds is from 0 to 4294967295. The range for milliseconds is from 0 to 999. If using milliseconds only, specify the milliseconds in the format 0.mmm.
maxrun	(Optional) Specifies the maximum runtime of the applet. If the **maxrun** keyword is specified, the *maxruntime-number* value must be specified. If the **maxrun** keyword is not specified, the default applet run time is 20 seconds.
maxruntime-number	(Optional) Number of seconds specified in ssssssss[.mmm] format, where ssssssss must be an integer representing seconds between 0 and 31536000, inclusive, and where mmm must be an integer representing milliseconds between 0 and 999).
ratelimit	(Optional) Specifies the ratelimit time interval of the applet. If the **ratelimit** keyword is specified, the *ratelimit-number* value must be specified.
ratelimit-number	(Optional) Number of seconds specified in ssssssss [*mmm*] format, where ssssssss must be an integer representing seconds from 0 to 31536000, and where *mmm* must be an integer representing milliseconds from 0 to 999.

Command Default

No EEM events are triggered on the basis of matches with syslog messages.

Command Modes

Applet configuration (config-applet)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE event syslog command.

Examples

The following example shows how to specify an EEM applet to run when the syslog identifies that Ethernet interface 1/0 is down. The applet sends a message about the interface to the syslog.

```
Device(config)# event manager applet interface-down
Device(config-applet)#  event syslog pattern {.*UPDOWN.*Ethernet1/0.*} occurs 4
```

event timer

To specify the event criteria for an Embedded Event Manager (EEM) applet that is run based on time-specific events, use the **event timer** command in applet configuration mode. To remove the time-specific event criteria, use the **no** form of this command.

event timer { **cron** [**cron-entry** *cron-entry* | **maxrun** *maxrun-number* | **name** *timer-name* | **ratelimit** *ratelimit-number*] | **watchdog** [**maxrun** *maxrun-number* | **name** *timer-name* | **ratelimit** *ratelimit-number* | **time** *time-value*] }
no event timer

Syntax Description

cron	Specifies that an event is triggered when the CRON string specification matches the current time.
cron-entry	Specifies the first five fields of a UNIX crontab entry as used with the UNIX CRON daemon.
cron-entry	Text string that consists of five fields separated by spaces. The fields represent the times and dates when CRON timer events will be triggered. Fields and corresponding values are as follows: • *minute*: A number in the range from 0 to 59 that specifies when a CRON timer event is triggered. • *hour*: A number in the range from 0 to 23 that specifies when a CRON timer event is triggered. • *day-of-month*: A number in the range from 1 to 31 that specifies the day of the month when a CRON timer event is triggered. • *month*: A number in the range from 1 to 12 or the first three letters (not case-sensitive) of the name of the month in which a CRON timer event is triggered. • *day-of-week*: A number in the range from 0 to 6 (Sunday is 0) or the first three letters (not case-sensitive) of the name of the day when a CRON timer event is triggered. Instead of the first five fields, special strings can be entered. See the "Usage Guidelines" section for details.
watchdog	Specifies that an event is triggered when the specified time counts down to zero. The timer automatically resets to the initial value and continues to count down.
name	(Optional) Specifies that the timer is named.

timer-name	(Optional) Name of the timer.
maxrun	(Optional) Specifies the maximum runtime of the applet. If the maxrun keyword is specified, the maxruntime-number value must be specified. If the maxrun keyword is not specified, the default applet run time is 20 seconds.
maxruntime-number	(Optional) Number of seconds specified in ssssssss[.mmm] format, where ssssssss must be an integer representing seconds between 0 and 31536000, inclusive, and where mmm must be an integer representing milliseconds between 0 and 999).
ratelimit	(Optional) Specifies the ratelimit time interval of the applet. If the **ratelimit** keyword is specified, the *ratelimit-number* value must be specified.
ratelimit-number	(Optional) Number of seconds specified in *ssssssss* [*mmm*] format, where *ssssssss* must be an integer representing seconds from 0 to 31536000, and where *mmm* must be an integer representing milliseconds from 0 to 999.
time	Specifies the time interval during which the event must take place.
time-value	Integer that specifies, in seconds and optional milliseconds, the time interval during which the event must take place. The range for seconds is from 0 to 4294967295 and the range for milliseconds is from 0 to 999. The format is ssssss[.mmm]. When only milliseconds are specified, use the format 0.mmm.

Command Default

No EEM events are triggered on the basis of time-specific events.

Command Modes

Applet configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE event timer command.

Examples

The following example shows how to specify that an event is triggered at 1:01 a.m. on January 1 each year:

```
Device(config)# event manager applet timer-cron1
Device(config-applet)# event timer cron cron-entry 1 1 1 1 * name Jan1
```

The following example shows how to specify that an event is triggered at noon on Monday through Friday of every week:

```
Device(config)# event manager applet timer-cron2
Device(config-applet)# event timer cron cron-entry 0 12 * * 1-5 name MonFri
```

The following example shows how to specify that an event is triggered at midnight on Sunday every week:

```
Device(config)# event manager applet timer-cron3
Device(config-applet)# event timer cron cron-entry @weekly name Sunday
```

The following example shows how to specify that an event is triggered every 5 hours:

```
Device(config)# event manager applet timer-watch
Device(config-applet)# event timer watchdog time 18000
```

event track

To specify the event criteria for an Embedded Event Manager (EEM) applet that is run based on a Cisco IOS Object Tracking subsystem report for the specified object number, use the **event track** command in applet configuration mode. To remove the report event criteria, use the **no** form of this command.

event track *object-number* [**state** { **up** | **down** | **any** }] [**maxrun** *maxruntime-number*] [**ratelimit** *ratelimit-number*]
no event track *object-number*

Syntax Description

object-number	Tracked object number in the range from 1 to 500, inclusive. The number is defined using the **track stub** command.
state	(Optional) Specifies that the tracked object transition will cause an event to be raised.
up	(Optional) Specifies that an event will be raised when the tracked object transitions from a down state to an up state.
down	(Optional) Specifies that an event will be raised when the tracked object transitions from an up state to a down state.
any	(Optional) Specifies that an event will be raised when the tracked object transitions to or from any state. This is the default.
maxrun	(Optional) Specifies the maximum runtime of the applet. If the **maxrun** keyword is specified, the *maxruntime-number* value must be specified. If the **maxrun** keyword is not specified, the default applet run time is 20 seconds.
maxruntime-number	(Optional) Number of seconds specified in ssssssss[.mmm] format, where ssssssss must be an integer representing seconds between 0 and 31536000, inclusive, and where mmm must be an integer representing milliseconds between 0 and 999).
ratelimit	(Optional) Specifies the ratelimit time interval of the applet. If the **ratelimit** keyword is specified, the *ratelimit-number* value must be specified.
ratelimit-number	(Optional) Number of seconds specified in *ssssssss* [*mmm*] format, where *ssssssss* must be an integer representing seconds from 0 to 31536000, and where *mmm* must be an integer representing milliseconds from 0 to 999.

Command Default

No EEM event criteria are specified.

Command Modes

Applet configuration (config-applet)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

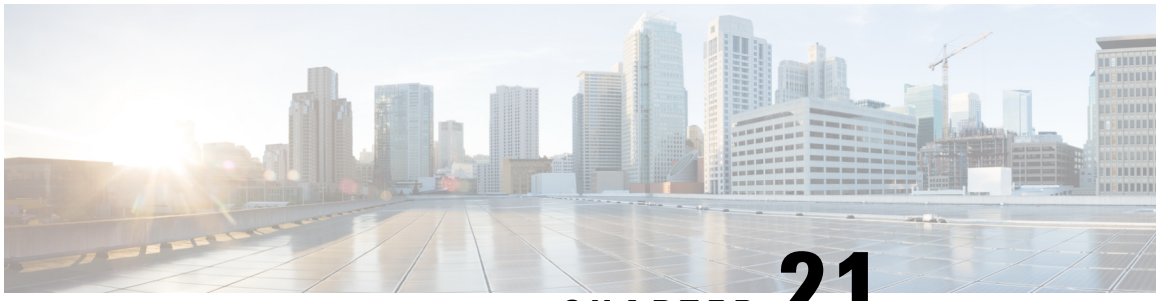
Usage Guidelines

For usage guidelines, see the Cisco IOS XE event track command.

Examples

The following example shows how to specify event criteria based on a tracked object:

```
Device(config)# event manager applet track-ten
Device(config-applet)# event track 10 state any
Device(config-applet)# action 1.0 track set 10 state up
Device(config-applet)# action 2.0 track read 10
```



CHAPTER 21

Frame-Relay-Native Commands

- frame-relay lmi-type , on page 255
- frame-relay intf-type, on page 256
- frame-relay interface-dlci, on page 257
- frame-relay multilink bandwidth-class, on page 258
- interface, on page 259
- interface MFR, on page 262
- ip address, on page 263
- encapsulation frame-relay, on page 264

frame-relay lmi-type

To select the Local Management Interface (LMI) type, use the **frame-relay lmi-type** command in interface configuration mode. To return to the default LMI type, use the **no** form of this command.

frame-relay lmi-type { **ansi** }
no frame-relay lmi-type { **ansi** }

Syntax Description

ansi	Annex D defined by American National Standards Institute (ANSI) standard T1.617.

Command Default

LMI autosense is active and determines the LMI type by communicating with the switch.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE frame-relay lmi-type command.

Examples

The following is an example of the commands you might enter to configure an interface for the ANSI Annex D LMI type:

```
interface Serial 0/1/0
encapsulation frame-relay
frame-relay lmi-type ansi
```

frame-relay intf-type

To configure a Frame Relay switch type, use the **frame-relay intf-type** command in interface configuration mode. To disable the switch, use the **no** form of this command.

frame-relay intf-type [dce | dte]
no frame-relay intf-type [dce | dte]

Syntax Description

dce	(Optional) Router or access server functions as a switch connected to a router.
dte	(Optional) Router or access server is connected to a Frame Relay network.

Command Default

The router or access server is connected to a Frame Relay network.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE frame-relay intf-type command.

Examples

The following example configures a DTE switch type:

```
interface Serial 0/1/0
frame-relay intf-type dte
```

Examples

The following example configures a DCE switch type on interface serial 0/0/1:5:

```
interface Serial 0/0/1:5
frame-relay intf-type dce
```

Examples

The following example configures a DTE switch type on MFR interface 1:

```
interface MFR1
frame-relay intf-type dte
```

frame-relay interface-dlci

To assign a data-link connection identifier (DLCI) to a specified Frame Relay subinterface on the router or access server, to assign a specific permanent virtual circuit (PVC) to a DLCI, use the **frame-relay interface-dlci** command in interface configuration mode. To remove this assignment, use the **no** form of this command.

frame-relay interface-dlci *dlci*
no frame-relay interface-dlci *dlci*

Syntax Description

dlci	DLCI number to be used on the specified subinterface. Range: 16-1007

Command Default

No DLCI is assigned.

Command Modes

Interface configuration (config-if)
Subinterface configuration (config-subif)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE frame-relay interface-dlci command.

Examples

The following example assigns DLCI 80 to the main interface and then removes it.

```
Router(config)# interface Serial 0/1/0
Router(config-if)# frame-relay interface-dlci 80
Router(config-fr-dlci)# exit
Router(config-if)# interface Serial 0/1/0
Router(config-if)# no frame-relay interface-dlci 80
```

The following example assigns DLCI 100 to a point-to-point serial interface.

```
Router(config)# interface Serial 0/1/0.2
Router(config-if)# encapsulation frame-relay ietf
Router(config-if)# frame-relay interface-dlci 100
```

The following example assigns DLCI 100 on MFR interface 1:

```
Router(config)# interface MFR1
Router(config-if)# frame-relay interface-dlci 100
```

frame-relay multilink bandwidth-class

To specify the criterion used to activate or deactivate a Frame Relay bundle, use the **frame-relay multilink bandwidth-class** command in interface configuration mode. To reset the bandwidth class to the default, use the **no** form of this command.

frame-relay multilink bandwidth-class { **a** | **b** | **c** }
no frame-relay multilink bandwidth-class

Syntax Description

a	Bandwidth class A (single link) criterion will be used to activate or deactivate the Frame Relay bundle. This is the default. • Criterion for activation--One or more bundle links indicate (by issuing a BL_ACTIVATE message) that operational bandwidth is available. When this occurs, the bundle emulates a physical link by issuing a PH_ACTIVATE message to the data-link layer. • Criterion for deactivation--All bundle links are down and issue a BL_DEACTIVATE message, which triggers a PH_DEACTIVATE message to be sent to the data-link layer, indicating that the Frame Relay bundle cannot accept frames.
b	Bandwidth class B (all links) criterion will be used to activate or deactivate the Frame Relay bundle. • Criterion for activation--All bundle links indicate (by issuing a BL_ACTIVATE message) that operational bandwidth is available. When this occurs, the bundle emulates a physical link by issuing a PH_ACTIVATE message to the data-link layer. • Criterion for deactivation--Any bundle link is down and issues a BL_DEACTIVATE message, which triggers a PH_DEACTIVATE message to be sent to the data-link layer, indicating that the Frame Relay bundle cannot accept frames.
c	Bandwidth class C (threshold) criterion will be used to activate or deactivate the Frame Relay bundle. • Criterion for activation--The minimum number of links in the configured bundle issue a BL_ACTIVATE message. When this occurs, the bundle emulates a physical link by issuing a PH_ACTIVATE message to the data-link layer. • Criterion for deactivation--The number of bundle links issuing a BL_ACTIVATE message falls below the configured *threshold* value. When this occurs, a PH_DEACTIVATE message is sent to the data-link layer, which indicates that the Frame Relay bundle cannot accept frames.

Command Default

Frame Relay bundles use bandwidth class A (single link).

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE frame-relay multilink bandwidth-class command.

Examples

The following example shows how to specify the class A (single link) bandwidth class to trigger activation or deactivation of the Frame Relay bundle on MFR interface 1:

```
interface MFR1
 frame-relay multilink bandwidth-class a
```

The following example shows how to specify the class B (all links) bandwidth class to trigger activation or deactivation of the Frame Relay bundle on MFR interface 1:

```
interface MFR1
 frame-relay multilink bandwidth-class b
```

The following example shows how to specify the class C (threshold) bandwidth class to trigger activation or deactivation of the Frame Relay bundle on MFR interface 1:

```
interface MFR1
 frame-relay multilink bandwidth-class c
```

interface

To configure an interface type and to enter interface configuration mode, use the **interface** command in the global configuration mode.

interface *type* *number* **.** *subinterface-number*

interface *type* *slot* / *subslot* / *port* **.** *subinterface-number* [**point-to-point**]

no interface *type* *number* **.** *subinterface-number*

no interface *type* *slot* / *subslot* / *port* **.** *subinterface-number* [**point-to-point**]

Syntax Description

type	Type of interface to be configured. See the table below.
number	Port, connector, or interface card number. The numbers are assigned at the factory at the time of installation or when added to a system; they can be displayed with the **showinterfaces** command.
slot	Chassis slot number. Refer to the appropriate hardware manual for slot information. For SIPs, refer to the platform-specific SPA hardware installation guide or the corresponding "Identifying Slots and Subslots for SIPs and SPAs" topic in the platform-specific SPA software configuration guide.
/ *subslot*	Secondary slot number on a SIP where a SPA is installed. The slash (/) is required. Refer to the platform-specific SPA hardware installation guide and the corresponding "Specifying the Interface Address on a SPA" topic in the platform-specific SPA software configuration guide for subslot information.

/ *port*	Port or interface number. Theslash(/)is required. Refer to the appropriate hardware manual for port information. For SPAs, refer to the corresponding “Specifying the Interface Address on a SPA” topics in the platform-specific SPA software configuration guide.
. *subinterface-number*	Subinterface number in the range 1 to 4294967293. The number that precedes the period (.) must match the number to which this subinterface belongs.
point-to-point	(Optional) Specifies a point-to-point subinterface.

Command Default

No interface types are configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release Amsterdam 17.2.1v	Commands of the following form were qualified for use in Cisco vManage CLI templates: • **interface ATM 0/3/0** • **interface ATM 0/3/0.1 point-to-point** • **interface Dialer 1** • **interface GigabitEthernet 1** • **interface GigabitEthernet 1.101** • **interface Loopback 100** • **interface Tunnel 10** • **interface VirtualPortGroup 0** • **interface Vlan 1**
Cisco IOS XE Release Amsterdam 17.3.1	Commands of the following form were qualified for use in Cisco vManage CLI templates: • **interface Serial 2/0** • **interface Serial 0/1/0** • **interface Serial 0/1/0.2 point-to-point**

Usage Guidelines

The table below displays the keywords that represent the types of interfaces that can be configured with the **interface** command. Replace the *type* argument with the appropriate keyword from the table.

When you want to push a CLI template or add on CLI template after an upgrade, to match the device running configuration, you must come out of the interface configuration. In this case, interface block must end with statement **exit** instead of "!". After configuring the interfaces, before starting on a new feature configuration, exit from the interface configuration mode.

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.15.1a, size limit for interface is within the range 1 to 31 for interface commands.

Usage Guidelines

Table 16: Interface Type Keywords

Keyword	Interface Type
ATM	ATM interface.
Dialer	Dialer interface.
GigabitEthernet	1000-Mbps Ethernet interface.
Loopback	Software-only loopback interface that emulates an interface that is always up. It is a virtual interface supported on all platforms. The *number* argument is the number of the loopback interface that you want to create or configure. There is no limit on the number of loopback interfaces that you can create.
Serial	Serial interface.
Tunnel	Tunnel interface; a virtual interface. The *number* argument is the number of the tunnel interface that you want to create or configure. There is no limit on the number of tunnel interfaces that you can create.
Vlan	VLAN interface.
VirtualPortGroup	Virtual Port Group interface.

For more usage guidelines, see interface.

ATM Interface

```
Device(config)# interface ATM 0/3/0
Device(config-if)#
```

```
Device(config)# interface ATM 0/3/0.1 point-to-point
Device(config-if)#
```

Dialer Interface

```
Device(config)# interface Dialer 1
Device(config-if)#
```

GigabitEthernet Interface

```
Device(config)# interface GigabitEthernet 1
Device(config-if)#
```

```
Device(config)# interface GigabitEthernet 1.101
Device(config-if)#
```

Loopback Interface

```
Router(config)# interface Loopback 100
Router(config-if)#
```

Serial Interface

```
Router(config)# interface Serial 2/0
Router(config-if)#

Router(config)# interface Serial 0/1/0
Router(config-if)#

Router(config)# interface Serial 0/1/0.2 point-to-point
Router(config-if)#

Router(config)# interface Serial 0/0/1:5
Router(config-if)#
```

Tunnel Interface

```
Router(config)# interface Tunnel 10
Router(config-if)#
```

Virtual Port Group Interface

```
Router(config)# interface VirtualPortGroup 0
Router(config-if)#
```

VLAN Interface

```
Router(config)# interface Vlan 1
Router(config-if)#
```

interface MFR

To configure a multilink Frame Relay bundle interface, use the **interface MFR** command in global configuration mode. To remove the bundle interface, use the **no** form of this command.

interface MFR *number*
no interface MFR *number*

Syntax Description

number	Number that will uniquely identify this bundle interface. Range: 0 to 2147483647.

Command Default

A Frame Relay bundle interface is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE interface MFR command.

Examples

The following example shows the configuration of a bundle interface called “MFR 1.”

```
interface MFR1
```

ip address

To set a primary or secondary IP address for an interface, use the **ip address** command in interface or sub-interface configuration mode. To remove an IP address or disable IP processing, use the **no** form of this command.

ip address *ip-address* [*mask*]
no ip address [*ip-address*] [*mask*]

Syntax Description

ip-address	IP address.
mask	(Optional) Mask for the associated IP subnet.

Command Default

No IP address is defined for the interface.

Command Modes

Interface configuration (config-if)

Sub-interface configuration (config-subif)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For the usage guidelines, see the Cisco IOS XE ip address command.

Examples

```
Device(config)# interface ATM 0/3/0.1 point-to-point

Device(config-if)# ip address 192.10.6.5

Device(config)# interface ATM 0/3/0.1

Device(config-subif)# ip address 10.0.0.0 255.255.255.252
```

```
Device(config)# interface Serial 0/1/0.2
Device(config-if)# ip address 10.1.1.1 255.255.255.0
Device(config)# interface Serial 0/0/1:5
Device(config-if)# ip address 10.1.1.1 255.255.255.0
Device(config)# interface MFR1
Device(config-if)# ip address 10.4.4.4 255.255.255.0
```

encapsulation frame-relay

To enable Frame Relay encapsulation, use the **encapsulation frame-relay** command in interface configuration mode. To disable Frame Relay encapsulation, use the **no** form of this command.

encapsulation frame-relay [**ietf**]
no encapsulation frame-relay [**ietf**]

Syntax Description

ietf	(Optional) Sets the encapsulation method to comply with the Internet Engineering Task Force (IETF) standard (RFC 1490). Use this keyword when connecting to another vendor's equipment across a Frame Relay network.

Command Default

The default is the encapsulation of Cisco.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE encapsulation frame-relay command.

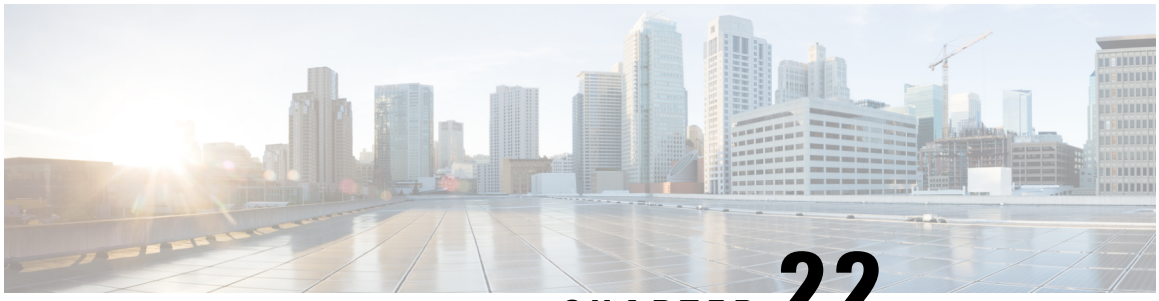
Examples

In the following example, use the **ietf** keyword if your router or access server is connected to another vendor's equipment across a Frame Relay network to confirm with RFC 1490:

```
interface Serial 0/1/0
encapsulation frame-relay ietf
```

The following example configures Cisco Frame Relay encapsulation on interface serial 0/0/1:5:

```
interface Serial 0/0/1:5
encapsulation frame-relay
```



CHAPTER 22

Global Configuration Commands

- clock, on page 265
- config-transaction, on page 266
- crypto isakmp diagnose error, on page 267
- hostname, on page 268
- line, on page 268
- login authentication, on page 269
- login on-success log, on page 270
- mac address-table aging-time, on page 271
- mac address-table static, on page 272
- memory free low-watermark processor, on page 272
- platform qfp utilization monitor load, on page 273
- platform-resource, on page 274
- sdwan, on page 274
- service password-recovery, on page 275
- service tcp-small-servers, on page 275
- service timestamps, on page 276
- service udp-small-servers, on page 278
- speed, on page 279
- speedtest disable-backward-compatible-ip, on page 279
- stopbits, on page 280
- transport input, on page 281
- transport output, on page 281
- username, on page 282

clock

Set the timezone to use on the local device.

clock timezone *timezone hours-offset*

Syntax Description

timezone *timezone*	Set the timezone on the device. *timezone* is one of the timezones in the tz database (also called tzdata, the zoneinfo database, or the IANA timezone database). Default: UTC
hours-offset	Hours offset from Coordinated Universal Time (UTC). Range is from –23 to +23.

Command Default

UTC

Command Modes

Global configuration (config)

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE clock timezone command.

Examples

```
Device(config)# clock timezone UTC 20
```

config-transaction

To enter global configuration mode on a Cisco IOS XE Catalyst SD-WAN device, use the **config-transaction** command in privileged EXEC mode.

config-transaction

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Use this command to enter global configuration mode on a Cisco IOS XE Catalyst SD-WAN device. Commands entered in this mode are written to the running configuration file, but saved in the running config after commit.

Example

The following example shows how to enter global configuration mode from privileged EXEC and set an ip address for a name server, then commit changes.

```
Device# config-transaction
Device(config)# ip name-server 10.255.1.1
Device(config)# commit
```

Table 17: Related Commands

Commands	Description
commit	Submits changes and writes to memory.
end	Cancels and exits out to privileged EXEC mode.
yes	Sends yes.
no	Sends no.
cancel	Cancels changes.

crypto isakmp diagnose error

To set the count of display errors for Internet Security Association and Key Management Protocol (ISAKMP), use the **crypto isakmp diagnose error** command in global configuration mode. To remove the ISAKMP error count, use the **no** form of this command.

crypto isakmp diagnose error *count*
no crypto isakmp diagnose error *count*

Syntax Description

count	Sets error counters.

Command Default

ISAKMP error diagnostic is enabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

IKE is a hybrid protocol that implements the Oakley key exchange and key exchange inside the framework. IKE is a key management protocol standard that is used in conjunction to configure basic VPNs. IPsec can be configured without IKE, but IKE enhances IPsec by providing additional features, flexibility, and ease of configuration for the IPsec standard.

Example

The following example shows how to configure the crypto diagnose error count to 10.

```
Device(config)# crypto isakmp diagnose error 10
```

hostname

To specify or modify the hostname for the network server, use the **hostname** command in global configuration mode.

hostname *name*

Syntax Description

name	New hostname for the network server.

Command Default

The default hostname is Router.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE hostname command.

line

To identify a specific line for configuration and enter line configuration collection mode, use the **line** command in global configuration mode. To remove configuration from a specific line, use the **no** form of this command.

line { **auto-consolidation** | **aux** | **con 0** | **range** | **vty** *line-number* }
no line { **auto-consolidation aux** | **con 0** | **range** | **vty** *line-number* }

auto-consolidation	Enable or disable auto-consolidation of terminal lines.
aux	(Optional) Auxiliary EIA/TIA-232 DTE port. Must be addressed as relative line 0. The auxiliary port can be used for modem support and asynchronous connections.
con 0	Console 0 terminal line. The console port is DCE.
vty	Virtual terminal line for remote console access.
range	Range of lines with first line number and last line number.

line-number	Relative number of the virtual terminal line (or the first line in a contiguous group) that you want to configure when the line type is specified. Numbering begins with zero. You can either configure a single line or a range.

Command Default

There is no default line.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	Additional parameters qualified: **auto-consolidation**, **aux** and **range**.
Cisco IOS XE Catalyst SD-WAN Release 26.2.1	**aux** parameter is not supported.

Usage Guidelines

From Cisco IOS XE Catalyst SD-WAN Release 26.2.1, **aux** parameter is unsupported. During an upgrade, SD-WAN Manager handles this command automatically.

For usage guidelines, see the Cisco IOS line command.

Examples

The terminal from which you locally configure the router is attached to the console port. To configure line parameters for the console port, enter the following:

```
line console 0
```

The following example starts configuration for virtual terminal lines 0 to 4:

```
line vty 0 4
```

The following example configuration shows how to disable auto-consolidation:

```
line auto-consolidation
```

To configure line parameters for the auxiliary port, enter the following:

```
line aux 0
```

The following example starts configuration for a range of lines:

```
line range 1 5
```

login authentication

To enable authentication, authorization, and accounting (AAA) authentication for logins, use the **login authentication**command inline configuration mode. To return to the default specified by the aaa authentication login command, use the **no** form of this command.

login authentication { **default** }
no login authentication { **default** }

Syntax Description

default	Uses the default list created with the **aaa authentication login** command.

Command Default

Uses the default set with **aaa authentication login**.

Command Modes

Line configuration (config-line)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1r	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

Note The default option for **login authentication** command is available only if you enter the line configuration mode using the **line console** command.

For usage guidelines, see the Cisco IOS XE login authentication command.

Examples

The following example specifies that the default AAA authentication is to be used on the line:

```
line con 0
 login authentication default
```

login on-success log

To generate a syslog message for successful login attempts, use the **login on-success log** command in global configuration mode. To remove the syslog setting, use the **no** form of this command.

login on-success log [**every** *number*]
no login on-success log [**every** *number*]

Syntax Description

every	Optional command.
number	The number of successful login attempts. The range is from 0 to 65535.

Command Default

Every successful login attempt is logged.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines Use the **login on-success log** command to generate a syslog message on every successful login attempt, or on any number of successful logins attempts up to 65535.

Example

The following example shows how to configure the syslog message to log every 10th successful login attempt.

```
Device(config)# login on-success log every 10
```

Table 18: Related Commands

Commands	Description
login on-success log	Logs every successful login.

mac address-table aging-time

To configure the maximum aging time for entries in the Layer 2 table, use the **mac address-tableaging-time** command in global configuration mode. To reset maximum aging time to the default setting, use the **no** form of this command.

mac address-table aging-time *seconds*
no mac-address-table aging-time *seconds*

Syntax Description

seconds	MAC address table entry maximum age. Aging time is counted from the last time that the switch detected the MAC address. The default value is 300 seconds.

Command Default The default aging time is 300 seconds.

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines The aging time entry will take the specified value. Valid entries are from 10 to 1000000 seconds.

This command cannot be disabled.

The following example shows how to configure aging time to 300 seconds:

```
mac address-table aging-time 300
```

mac address-table static

To add static entries to the MAC address table or to disable Internet Group Multicast Protocol (IGMP) snooping for a particular static multicast MAC address, use the **mac address-table static** command in global configuration mode. To remove entries profiled by the combination of specified entry information, use the **no** form of this command.

mac address-table static *mac-address* **vlan** *vlan-id* **interface** *type slot / port*
no mac-address-table static *mac-address* **vlan** *vlan-id* **interface** *type slot/port*

Syntax Description

mac-aadress	Address to add to the MAC address table.
vlan *vlan-id*	Specifies the VLAN associated with the MAC address entry. The range is from 2 to 100.
interface *type slot/port* or **interface** *type number*	Specifies the interface type and the slot and port to be configured. On the Catalyst switches, the*type* and *number* arguments should specify the interface type and the *slot/port* or *slot/subslot/port* numbers (for example, **interface pos 5/0** or **interface ATM 8/0/1**).

Command Default

Static entries are not added to the MAC address table.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE mac address-table static command.

Examples

The following example shows how to add static entries to the MAC address table:

```
Device(config)# mac-address-table static 0050.3e8d.6400 vlan 100 interface fastethernet5/7
```

memory free low-watermark processor

To set a low free memory threshold, use the **memory free low-watermark processor** command in global configuration mode. To remove a low free memory threshold, use the **no** form of this command.

memory free low-watermark processor *threshold*

Syntax Description

threshold	Specifies threshold in kilobytes of free processor. The range is from 0 to 4294967295.

Command Default None

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines When a router is overloaded by processes, the amount of available memory might fall to levels insufficient for it to issue critical notifications. Use the **memory free low-watermark processor** command to reserve a region of memory to be used by the router for issuing critical notifications.

Example

The following example shows how to configure a memory threshold for the router.

```
Device(config)# memory free low-watermark processor 70694
```

platform qfp utilization monitor load

To set the default value for CPU utilization monitoring, use the **platform qfp utilization monitor load** command in global configuration mode. To remove the platform qfp utilization monitor load, use the **no** form of this command.

platform qfp utilization monitor load *load*

Syntax Description

load	The range is from 0 to 65535, and from range 50 to 90 can be either set to Packets Per Second (PPS) or a percent.

Command Default The default value for this command is set to 80%.

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines The qfp monitoring is set to 80 percent by default, therefore when the CPU is running at 80 percent or above it will start to log warning and error messages. This default value can be changed to a smaller/larger percent or globally.

Example

The following examples shows how to configure a platform qfp utilization monitor load value to 75% and 60535 pps.

```
Device(config)# platform qfp utilization monitor load 75
Device(config)# platform qfp utilization monitor load 60535
```

platform-resource

To select a template for core allocation, use the **platform-resource** command in configuration mode. To remove this configuration, use the **no** form of this command.

platform-resource [**service-plane-heavy** | **data-plane-heavy**]

no platform-resource

Syntax Description

service-plane-heavy	(Optional) Specifies using service plane heavy template.
data-plane-heavy	(Optional) Specifies using data plane heavy template.

Command Default Platform resource template is not configured.

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco vManage CLI templates.

The following example shows how to configure vCPU distribution across the service plane.

```
Device(config)# platform resource service-plane-heavy
```

sdwan

To enter the SD-WAN configuration mode (config-sdwan) on a Cisco IOS XE SD-WAN device, enter the **sdwan** command in the global configuration mode.

sdwan

Syntax Description This comand has no keywords or arguments.

Command Default None

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

Example

```
Device# config-transaction
Device(config)# sdwan
```

service password-recovery

To enable password recovery capability, use the **service password-recovery** command in global configuration mode. To disable password recovery capability, use the **no service password-recovery [strict]** command.

service password-recovery
no service password-recovery [strict]

Syntax Description

[strict]	(Optional) Restricts device recovery.

Command Default

Password recovery capability is enabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Release 17.6.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE service password-recovery command.

Example

The following example shows how to disable password recovery capability using the **no service password-recovery strict** command:

```
Device# configure terminal
Device(config)# no service password-recovery strict
WARNING:
Executing this command will disable the password recovery mechanism.
Do not execute this command without another plan for password recovery.
Are you sure you want to continue? [yes]: yes
.
.
```

service tcp-small-servers

To enable small TCP servers such as the Echo, use the **service tcp-small-servers** command in global configuration mode. To disable the TCP server, use the **no** form of this command.

service tcp-small-servers

no service tcp-small-servers

Command Default

TCP small servers are disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE service tcp small servers command.

Examples

The following example shows how to enable small TCP servers:

```
Device(config)# service tcp-small-servers
```

service timestamps

To configure the system to apply a time stamp to debugging messages or system logging messages, use the **service timestamps** command in global configuration mode. To disable this service, use the **no** form of this command.

service timestamps [**debug** | **log**] [**uptime** | **datetime** *msec*] [**localtime**] [**show-timezone**] [**year**]
no service timestamps [**debug** | **log**]

Syntax Description

debug	(Optional) Indicates time-stamping for debugging messages.
log	(Optional) Indicates time-stamping for system logging messages.
uptime	(Optional) Specifies that the time stamp should consist of the time since the system was last rebooted. For example “4w6d” (time since last reboot is 4 weeks and 6 days). • This is the default time-stamp format for both debugging messages and logging messages. • The format for uptime varies depending on how much time has elapsed: • *HHHH* :*MM* :*SS* (*HHHH* hours: *MM* minutes: *SS* seconds) for the first 24 hours • *D* d*HH* h (*D* days *HH* hours) after the first day • *W* w*D* d (*W* weeks *D* days) after the first week

datetime	(Optional) Specifies that the time stamp should consist of the date and time. • The time-stamp format for **datetime** is MMM DD HH:MM:SS, where MMM is the month, DD is the date, HH is the hour (in 24-hour notation), MM is the minute, and SS is the second. • If the datetime keyword is specified, you can optionally add the **msec localtime** , **show-timezone** , or **year** keywords. • If the **service timestamps datetime** command is used without addtional keywords, time stamps will be shown using UTC, without the year, without milliseconds, and without a time zone name.
msec	(Optional) Includes milliseconds in the time stamp, in the format *HH***:** *DD***:** *MM***:** *SS***.** *mmm* , where *.mmm* is milliseconds
localtime	(Optional) Time stamp relative to the local time zone.
year	(Optional) Include the year in the date-time format.
show-timezone	(Optional) Include the time zone name in the time stamp. **Note** If the localtime keyword option is not used (or if the local time zone has not been configured using the **clock timezone** command), time will be displayed in Coordinated Universal Time (UTC).

Command Default

Time stamps are applied to debug and logging messages.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Command qualified for use in Cisco vManage CLI templates.
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a Cisco IOS XE Catalyst SD-WAN Release 17.6.4 and later releases of 17.6.x	Added support for the **localtime**, **year**, and **show-timezone** options.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE service timestamps command.

Examples

In the following example, the router begins with time-stamping disabled. Then, the default time-stamping is enabled (uptime time stamps applied to debug output). Then, the default time-stamping for logging is enabled (uptime time stamps applied to logging output).

```
Router# show running-config | include time

no service timestamps debug uptime
no service timestamps log uptime
Router# config terminal
```

```
Device(config)# service timestamps

! issue the show running-config command in config mode using  do  Router(config)# do show
running-config | inc time

! shows that debug timestamping is enabled, log timestamping is disabled
service timestamps debug uptime
no service timestamps log uptime
! enable timestamps for logging messages
Router(config)# service timestamps log
Router(config)# do show run | inc time

service timestamps debug uptime
service timestamps log uptime
Router(config)# service sequence-numbers

Router(config)# end

000075: 5w0d: %SYS-5-CONFIG_I: Configured from console by console
! The following is a level 5 system logging message
! The leading number comes from the  service sequence-numbers command.
! 4w6d indicates the timestamp of 4 weeks, 6 days 000075: 4w6d: %SYS-5-CONFIG_I: Configured
 from console by console
```

In the following example, the user enables time-stamping on logging messages using the current time and date in Coordinated Universal Time/Greenwich Mean Time (UTC/GMT), and enables the year to be shown.

```
Router(config)# service timestamps log datetime show-timezone year

Router(config)# end
! The following line shows the timestamp with datetime (11:13 PM March 22nd)
.Mar 22 2004 23:13:25 UTC: %SYS-5-CONFIG_I: Configured from console by console
```

service udp-small-servers

To enable small User Datagram Protocol (UDP) servers such as the Echo, use the **service udp-small-servers** command in global configuration mode. To disable the UDP server, use the **no** form of this command.

service udp-small-servers
no service udp-small-servers

Command Default

UDP small servers are disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE service udp small servers command.

Examples

The following example shows how to enable small UDP:

```
Router(config)# service udp-small-servers
```

speed

To configure the speed for a Fast Ethernet or Gigabit Ethernet interface, use the **speed** command in line configuration mode. To return to the default configuration, use the **no** form of this command.

speed *speed-range*
no speed *speed-range*

Syntax Description

speed-range	Configures the interface to transmit at the specified speed range.

Command Default

None

Command Modes

Line configuration (config-line)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE speed command.

Examples

The following is an example of this command

```
Device# configure terminal
Device(config)# line con 0
Device(config-line)# speed 9600
```

speedtest disable-backward-compatible-ip

To disable the 11.1.x.x IP address on the site-to-site speedtest loopback interface (Loopback65529), use the **speedtest disable-backward-compatible-ip** command in SD-WAN configuration mode. To restore the secondary 11.1.x.x address, use the **no** form of the command.

speedtest disable-backward-compatible-ip
no speedtest disable-backward-compatible-ip

Syntax Description

This command has no keywords or arguments.

Command Default

The 11.1.x.x IP address is enabled as a secondary address on Loopback65529 by default to maintain backward compatibility.

Command Modes

SDWAN Configuration (config-sdwan)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 26.1.1	Command introduced to support private IP addresses (10.1.x.x) for site-to-site speed tests and allow removal of 11.1.x.x.

Usage Guidelines

Use this command to remove 11.1.x.x IP address from the speedtest loopback interface.

When this command is configured:

- The 11.1.x.x secondary address is removed from Loopback65529.
- The device uses the private 10.1.x.x primary address for site-to-site speedtests.
- The device can no longer perform site-to-site speed tests with peer devices running older software versions that only support the 11.1.x.x address range.

Example

The following example shows how to disable the backward-compatible IP address for speedtest.

```
Device(config-sdwan)# speedtest disable-backward-compatible-ip
```

stopbits

To configure the stop bits for the console port, use the **stopbits** command. To revert to the default, use the **no** form of this command.

stopbits { **1** }

no stopbits { **1** }

Syntax Description

1	Specifies one stop bit.

Command Default

1 stop bit

Command Modes

Terminal line configuration mode (config)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1r	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

You can configure the console port only from a session on the console port.

Examples

This example shows how to configure the number of stop bits for the console port:

```
line con 0
stopbits 1
```

transport input

To define which protocols to use to connect to a specific line of the router, use the **transport input**command in line configuration mode. To change or remove the protocol, use the **no** form of this command.

transport input { **ssh** }

no transport input { **ssh** }

Syntax Description

ssh	(Optional) Selects the Secure Shell (SSH) protocol.

Command Default

No protocols are allowed on the auxiliary (AUX), console, tty, and vty lines.

Command Modes

Line configuration (config-line)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1r	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

Cisco devices do not accept incoming network connections to tty lines by default. You must specify an incoming transport protocol or specify the transport input all command before the line will accept incoming connections.

Examples

The following example shows you how to set the incoming protocol for the vty lines 0 to 32 to Telnet:

```
configure terminal
line vty 0 32
transport input ssh
exit
```

transport output

To determine the protocols that can be used for outgoing connections from a line, use the **transport output** command in line configuration mode. To change or remove the protocol, use the **no** form of this command.

transport output ssh

no transport output [**ssh**]

Syntax Description

ssh	Specifies the Secure Shell (SSH) protocol.

Command Default Telnet

Command Modes Line configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	Command qualified for use in Cisco vManage CLI templates.

Examples

The following example selects the SSH protocol:

```
transport output ssh
```

username

To establish a username-based authentication system, use the **username** command in global configuration mode. To remove an established username-based authentication, use the **no** form of this command.

username *name* [**privilege** *level* **secret** { **0** | **5** | **9** }]
no username *name*

Syntax Description

name	Hostname, server name, user ID, or command name. The *name* argument can be only one word. Blank spaces and quotation marks are not allowed.
0	Specifies that an unencrypted password or secret (depending on the configuration) follows.
5	Specifies that the type-5 encrypted password follows.
9	Specifies that the type-9 encrypted password follows.
secret	Specifies a secret for the user.
secret	For Challenge Handshake Authentication Protocol (CHAP) authentication: specifies the secret for the local router or the remote device. The secret is encrypted when it is stored on the local router. The secret can consist of any string of up to 11 ASCII characters. There is no limit to the number of username and password combinations that can be specified, allowing any number of remote devices to be authenticated.
privilege *privilege-level*	(Optional) Sets the privilege level for the user. Range: 0 to 15.

Command Default No username-based authentication system is established.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

The **username** command provides username or password authentication, or both, for login purposes only.

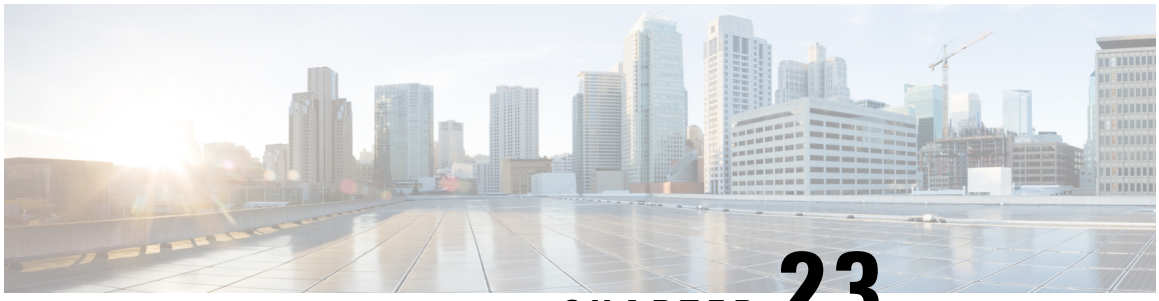
Examples

In the following example, a privilege level 1 user is denied access to privilege levels higher than 1:

```
username employee1 privilege 5
```

The following example shows how to create a local user named admin with admin1234 for a secret with (privilege 15).

```
Device(config)# username admin privilege 15 secret admin1234
```



CHAPTER 23

high-availability

- redundancy, on page 285
- application redundancy, on page 286
- preempt, on page 286
- init-role, on page 287
- path-optimization, on page 287
- redundancy rii, on page 288

redundancy

To configure the high availability feature on a Cisco IOS XE Catalyst SD-WAN device, use the **redundancy** command in global configuration mode. To disable redundancy, use the **no** form of this command.

redundancy

no redundancy

Command Default

No redundancy is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.15.1a	This command was introduced.

Examples

The following example shows how to configure redundancy for high availability on a Cisco IOS XE Catalyst SD-WAN device:

```
Device(config)# redundancy
```

application redundancy

To enable and manage the redundancy features for applications on a Cisco IOS XE Catalyst SD-WAN device, use the **application redundancy** command in application redundancy configuration mode. To disable redundancy, use the **no** form of this command.

application redundancy

no application redundancy

Command Default

No redundancy is configured.

Command Modes

Application redundancy (config-red)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.15.1a	This command was introduced.

Usage Guidelines

If the application is using redundancy like NAT, you cannot use **no application redundancy** to disable redundancy. It fails with error, % An application configuration exists on group. Hence, you need to remove redundancy configuration from application side before using **no application redundancy** .

Examples

The following example enables the redundancy feature for applications, allowing you to configure high availability settings on a Cisco IOS XE Catalyst SD-WAN device:

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

preempt

To enable preempt (allowing the standby device to automatically take over as the active device) for a redundancy group, use the **preempt** command in redundancy application group configuration mode. To disable redundancy, use the **no** form of this command.

preempt

no preempt

Command Default

No redundancy is configured.

Command Modes

Redundancy application group (config-red-app-grp)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.15.1a	This command was introduced.

Examples

The following example enables preemption on the redundancy group, allowing the standby device to automatically take over as the active device if it has a higher priority within the redundancy group:

```
Device(config-red-app-grp)# preempt
```

init-role

To specify the initial role of a redundancy group , use the **init-role** command in the application redundancy group configuration mode. To disable redundancy, use the **no** form of this command.

init-role
active | **standby**

no init-role
active | **standby**

Syntax Description

active	Sets the device to start as the active device in the redundancy group.
standby	Sets the device to start as the standby device in the redundancy group.

Command Default

No redundancy is configured.

Command Modes

application redundancy group configuration (config-app-redundancy-group)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.15.1a	This command was introduced.

Examples

The following example shows how to set the initial role of the redundancy group to active, ensuring the device starts as the active device upon initialization:

```
Device(config-app-redundancy-group)# init-role active
```

Examples

The following example shows how to set the initial role of the redundancy group to standby, ensuring the device starts as the standby device upon initialization:

```
Device(config-app-redundancy-group)# init-role standby
```

path-optimization

To enable path optimization feature, use the **path-optimization** command in global configuration mode. To disable redundancy, use the **no** form of this command.

path-optimization

no path-optimization

Command Default No redundancy is configured.

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.15.1a	This command was introduced.

Examples The following example shows how to enable the path optimization feature, allowing the device to dynamically adjust traffic paths for improved network performance:

```
Device(config)# path-optimization
```

redundancy rii

To assign a Redundancy Interface Identifier (RII) to a specific interface on a Cisco IOS XE Catalyst SD-WAN device, use the **redundancy rii** command in Interface configuration mode. To disable redundancy, use the **no** form of this command.

redundancy rii

no redundancy rii

Syntax Description

rii value	Specifies a unique identifier for an interface

Command Default No redundancy is configured.

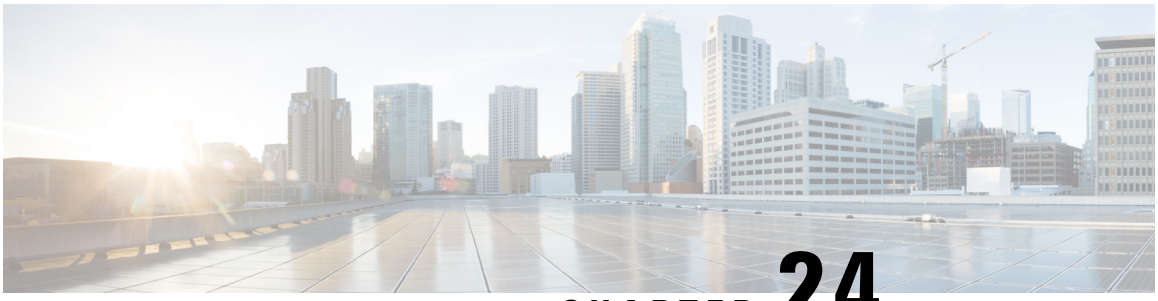
Command Modes Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.15.1a	This command was introduced.

Examples The following example shows the rii-value of 350 is assigned to the interface, uniquely identifying it within the redundancy group:

```
Device(config-if)# redundancy rii 350
```



CHAPTER 24

Hub and Spoke

- topology hub-and-spoke enable, on page 289

topology hub-and-spoke enable

Use the **topology hub-and-spoke enable** command in system configuration mode on a Cisco SD-WAN Controller to configure a hub-and-spoke topology in the network that the Cisco SD-WAN Controller is serving. Use the **no** form of the command to disable this method of configuring a hub-and-spoke topology.

topology hub-and-spoke enable

no topology hub-and-spoke enable

Command Default

By default, hub-and-spoke topology is not enabled on Cisco SD-WAN Controllers.

Command Modes

System configuration (config-system)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	This command was introduced.

Usage Guidelines

You can configure a hub-and-spoke topology using transport gateway to operate as hubs. The resulting hub-and-spoke topology applies to all VRFs. This method avoids the need for complex centralized control policy.

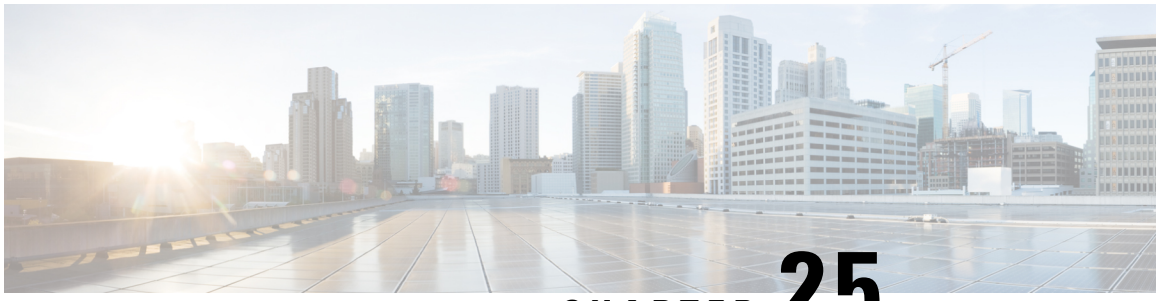
The configuration requires only a few simple configuration steps: a single command each on (a) the Cisco SD-WAN Controllers serving a network, (b) a router that serves as a hub, configured as a transport gateway, and (c) edge routers operating as spokes.

Example

```
sdwanController(config)#system
sdwanController(config-system)#topology hub-and-spoke enable
```

Related Commands

Command	Description
transport-gateway enable	A transport gateway operates as the hub in a hub-and-spoke routing topology. The **transport-gateway enable** command enables transport functionality on a router.
site-type	The **site-type** command configures the site type of a router. Site type is used in conjunction with transport gateway configuration.



CHAPTER 25

HSRP Commands

- standby authentication, on page 291
- standby follow, on page 293
- standby ip, on page 293
- standby ipv6, on page 294
- standby mac-address, on page 295
- standby mac-refresh, on page 296
- standby name, on page 296
- standby preempt, on page 297
- standby priority, on page 298
- standby timers, on page 299
- standby track, on page 300
- standby version, on page 302

standby authentication

To configure an authentication string for the Hot Standby Router Protocol (HSRP), use the **standby authentication** command in interface configuration mode. To delete an authentication string, use the **no** form of this command.

standby [*group-number*] **authentication** {**text** *string* | **md5** {**key-string** [**0** | **7** | **timeout** *seconds*] | **key-chain** *name-of-chain*}}
no standby [*group-number*] **authentication** {**text** *string* | **md5** {**key-string** [**0** | **7** | **timeout** *seconds*] | **key-chain** *name-of-chain*}}

Syntax Description

group-number	(Optional) Group number on the interface to which this authentication string applies. Range is from 0 to 65535. The default group number is 0.
text *string*	Specifies an authentication string. It can be up to eight characters long. The default string is *cisco*.
md5	Specifies Message Digest 5 (MD5) authentication.
key-string *key*	Specifies the secret key for MD5 authentication. The key can contain up to 64 characters. We recommend that you use at least 16 characters.

0	(Optional) Specifies an unencrypted key. If no prefix is specified, the text is also unencrypted.
7	(Optional) Specifies an encrypted key.
timeout *seconds*	(Optional) Duration, in seconds, that HSRP accepts message digests based on both the old and new keys.
key-chain *name-of-chain*	Identifies a group of authentication keys.

Command Default

No text authentication string is configured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE standby <*group-number*> authentication command.

Examples

The following example shows how to configure company1 as the authentication string required to allow hot standby routers in group 1 to interoperate:

```
interface GigabitEthernet 0/0/1
!
 standby 1 authentication text company1
!
```

The following example shows how to configure MD5 authentication using a key string named 345890:

```
interface GigabitEthernet 0/0/1
!
 standby 1 ip 10.21.0.12
 standby 1 priority 110
 standby 1 preempt
 standby 1 authentication md5 key-string 345890 timeout 30
!
```

The following example shows how to configure MD5 authentication using a key chain. HSRP queries the key chain “hsrp1” to obtain the current live key and key ID for the specified key chain:

```
key chain hsrp1
!
 key 1
!
 key-string 543210
 exit
!
 interface GigabitEthernet 0/0/1
!
 standby 1 ip 10.21.0.10
 standby 1 priority 110
 standby 1 preempt
 standby 1 authentication md5 key-chain hsrp1
!
```

standby follow

To configure an Hot Standby Router Protocol (HSRP) group to become an IP redundancy client of another HSRP group, use the **standby follow** command in interface configuration mode. To remove the configuration of an HSRP group as a client group, use the **no** form of this command.

standby *group-number* **follow** *group-name*
no standby *group-number* **follow** *group-name*

Syntax Description

group-number	Group number on the interface for which HSRP is being activated. Range is from 0 to 65535. The default is 0.
group-name	Name of the master group for the client group to follow.

Command Default

HSRP groups are not configured as client groups.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE standby <*group-number*> follow command.

Use the **show standby** command to display complete information about an HSRP client group.

Examples

The following example shows how to configure HSRP group 2 as a client to the HSRP1 master group:

```
interface GigabitEthernet 0/0/1
!
   standby 2 follow HSRP1
```

standby ip

To activate the Hot Standby Router Protocol (HSRP), use the **standby ip** command in interface configuration mode. To disable HSRP, use the **no** form of this command.

standby *group-number* **ip** [*ip-address* [**secondary**]]
no standby [*group-number*] **ip** [*ip-address*]

Syntax Description

group-number	(Optional) Group number on the interface for which HSRP is being activated. The default is 0. The group number range is from 0 to 255 for HSRP version 1 and from 0 to 4095 for HSRP version 2.
ip-address	(Optional) IP address of the hot standby router interface.

secondary	(Optional) Indicates that the IP address is a secondary Hot Standby router interface. Useful on interfaces with primary and secondary addresses; you can configure primary and secondary HSRP addresses.

Command Default

The default group number is 0. HSRP is disabled by default.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE standby <*group-number*> ip command.

Examples

The following example shows how to activate HSRP for group 1 on GigabitEthernet interface 0/0/1. The IP address used by the hot standby group is learned using HSRP:

```
interface GigabitEthernet 0/0/1
!
 standby 1 ip
```

The following example shows how all three virtual IP addresses appear in the Address Resolution Protocol (ARP) table using the same (single) virtual MAC address. All three virtual IP addresses are using the same HSRP group (group 1).

```
ip address 10.1.1.1 255.255.255.0
ip address 10.2.2.2 255.255.255.0 secondary
ip address 10.3.3.3 255.255.255.0 secondary
ip address 10.4.4.4 255.255.255.0 secondary
standby 1 ip 10.1.1.254
standby 1 ip 10.2.2.254 secondary
standby 1 ip 10.3.3.254 secondary
```

standby ipv6

To activate the Hot Standby Router Protocol (HSRP) in IPv6, use the **standby ipv6** command in interface configuration mode. To disable HSRP, use the **no** form of this command.

standby *group-number* **ipv6** { *link-local-ipv6-address* | **autoconfig** }
no standby *group-number* **ipv6** { *link-local-ipv6-address* | **autoconfig** }

Syntax Description

group-number	(Optional) Group number on the interface for which HSRP is being activated. The default is 0. The group number range is from 0 to 255 for HSRP version 1 and from 0 to 4095 for HSRP version 2.
link-local-ipv6-address	Link-local address of the hot standby router interface.

autoconfig	Indicates that a virtual link-local address is generated automatically from the link-local prefix and a modified EUI-64 format interface identifier, where the EUI-64 interface identifier is created from the relevant HSRP virtual MAC address.

Command Default

The default group number is 0. HSRP is disabled by default.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE standby <*group-number*> ipv6 command.

Examples

The following example shows how to enable an HSRP group for IPv6 operation:

```
Device(config)# standby version 2
Device(config)# interface GigabitEthernet0/0/1
Device(config-if)# standby ipv6 autoconfig
```

The following example shows how to configure an HSRP IPv6 address:

```
Device(config)# interface GigabitEthernet0/0/1
Device(config-if)# no ip address
Device(config-if)# ipv6 address FE80::233:33FF:FE33:3333
Device(config-if)# standby version 2
Device(config-if)# standby 110 ipv6 FE80::233:33FF:FE33:3333
```

standby mac-address

To specify a virtual MAC address for the Hot Standby Router Protocol (HSRP), use the **standby mac-address** command in interface configuration mode. To revert to the standard virtual MAC address (000.0C07.AC*xy*), use the **no** form of this command.

standby *group-number* **mac-address** *mac-address*
no standby *group-number* **mac-address**

Syntax Description

group-number	Group number on the interface for which HSRP is being activated. Range is from 0 to 65535. The default is 0.
mac-address	MAC address.

Command Default

If this command isn't configured, and the **standby use-bia** command isn't configured, the standard virtual MAC address—0000.0C07.AC*xy*, where *xy* is the group number in hexadecimal. This address is specified in RFC 2281, Cisco Hot Standby Router Protocol (HSRP).

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE standby <*group-number*> mac-address command.

Examples

The following example shows how to configure HSRP group 1 with the virtual MAC address, if the end nodes are configured to use 4000.1000.1060 as the MAC address of the network node:

```
Device(config)# interface GigabitEthernet 0/0/1
Device(config-if)# standby 1 ipv6 FE80::233:33FF:FE33:3333
Device(config-if)#  standby 1 mac-address 4000.1000.1060
```

standby mac-refresh

To change the interval at which packets are sent to refresh the MAC cache when the HSRP is running over FDDI, use the **standby mac-refresh** command in interface configuration mode. To restore the default value, use the **no** form of this command.

standby mac-refresh *seconds*
no standby mac-refresh

Syntax Description

seconds	Specifies the number of seconds in the interval at which a packet is sent to refresh the MAC cache. The maximum value is 255 seconds. The default is 10 seconds.

Command Default

The standby MAC refresh interval is 10 seconds.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE standby mac-refresh command.

Examples

The following example shows how to change the MAC refresh interval to 100 seconds. Therefore, a learning bridge would have to miss three packets before the entry gets timed out:

```
Device(config)# interface GigabitEthernet0/0/1
Device(config-if)# standby mac-refresh 100
```

standby name

To specify the name of the HSRP standby group, use the **standby name** command in interface configuration mode. To remove the name, use the **no** form of this command.

standby *group-number* **name** *group-name*
no standby *group-number* **name** *group-name*

Syntax Description

group-number	Specifies the group number on the interface to which this authentication string applies. Range is 0–65535. The default group number is 0.
group-name	Specifies the name of the standby group.

Command Default

The Hot Standby Router Protocol (HSRP) is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE standby <*group-number*> name command.

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.9.1a, static NAT mapping configurations with HSRP is supported. The redundancy naming conventions doesn't include spaces. We recommend that you do not use redundancy name with spaces while configuring **standby group-number name***[redundancy-name]* command.

Examples

The following example shows how to specify the standby name as SanJoseHA:

```
Device(config)# interface GigabitEthernet0/0/1
Device(config-if)# ip address 10.0.0.1 255.0.0.0
Device(config-if)# standby 1 ip 10.0.0.10
Device(config-if)# standby 1 name SanJoseHA
Device(config-if)# standby 1 preempt delay sync 100
Device(config-if)# standby 1 priority 110
```

standby preempt

To configure Hot Standby Router Protocol (HSRP) preemption and preemption delay, use the **standby preempt** command in interface configuration mode. To restore the default values, use the **no** form of this command.

standby *group-number* **preempt** [**delay** [**minimum** *seconds* | **reload** *seconds* | **sync** *seconds*]]
no standby *group-number* **preempt delay**

Syntax Description

group-number	Group number on the interface to which the other arguments in this command apply.
delay	(Optional) Specifies the delay duration. Required if either the **minimum**, **reload**, or **sync** keywords are specified.

minimum *seconds*	(Optional) Specifies the minimum delay period, in seconds. The *seconds* argument causes the local device to postpone taking over the active role for a minimum number of seconds since that device was last restarted. The range is from 0 to 3600 seconds (1 hour). The default is 0 seconds (no delay).
reload *seconds*	(Optional) Specifies the preemption delay, in seconds, after a reload. This delay period applies only to the first interface-up event after the device has reloaded, if such an event occurs within 360 seconds from reload. The timer starts at the interface-up event.
sync *seconds*	(Optional) Specifies the maximum synchronization period for IP redundancy clients in seconds.

Command Default

The default group number is 0. The default delay is 0 seconds. If the device wants to preempt, it does so immediately. By default, the device that comes up later becomes the standby.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE standby <*group-number*> preempt command.

Examples

The following example shows how to configure a minimum delay of 300 seconds (5 minutes). The device waits for 300 seconds (5 minutes) before attempting to become the active device:

```
Device(config)# interface GigabitEthernet0/0/1
Device(config-if)# standby 1 ip 172.19.108.254
Device(config-if)# standby 1 preempt delay minimum 300
```

standby priority

To configure Hot Standby Router Protocol (HSRP) priority, use the **standby priority** command in interface configuration mode. To restore the default values, use the **no** form of this command.

standby *group-number* **priority** *priority*
no standby *group-number* **priority** *priority*

Syntax Description

group-number	Group number on the interface to which the other arguments in this command apply. The default group number is 0.
priority	Priority value that prioritizes a potential hot standby router. The range is from 1 to 255, where 1 denotes the lowest priority and 255 denotes the highest priority. The default priority value is 100. The router in the HSRP group with the highest priority value becomes the active router.

Command Default

The default group number is 0. The default priority is 100.

Command Modes Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines For usage guidelines, see the Cisco IOS XE standby <*group-number*> priority command.

Examples The following example shows how to configure a priority of 120 (higher than the default value) to a router:

```
Device(config)# interface GigabitEthernet0/0/1
Device(config-if)# standby 1 ip 172.19.108.254
Device(config-if)# standby 1 priority 120
Device(config-if)# standby 1 preempt delay minimum 300
```

standby timers

To configure the time between hello packets and the time before other routers declare the active hot standby or standby router to be down, use the **standby timers** command in interface configuration mode. To restore the timers to their default values, use the **no** form of this command.

standby *group-number* **timers** [**msec**] *hellotime* [**msec**] *holdtime*
no standby *group-number* **timers** [**msec**] *hellotime* [**msec**] *holdtime*

Syntax Description

group-number	Group number on the interface to which the timers apply. The default is 0.
msec	(Optional) Timer interval, in milliseconds. (Millisecond timers allow for faster failover.)
hellotime	Hello interval, in seconds. This is an integer from 1 to 254. The default is 3 seconds. If the **msec** option is specified, the hello interval is in milliseconds. Valid value is from 15 to 999.
holdtime	Time, in seconds, before the active or standby router is declared to be down. This is an integer from *x* to 255. The default is 10 seconds. If the **msec** option is specified, *holdtime* is in milliseconds. Valid value is from *y* to 3000. • *x* is *hellotime* + 50 milliseconds, and then rounded up to the nearest 1 second • *y* is greater than or equal to three times *hellotime*, and is not less than 50 milliseconds.

Command Default The default group number is 0. The default hello interval is 3 seconds. The default hold time is 10 seconds.

Command Modes Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE standby <*group-number*> timers command.

Examples

The following example shows how to set the time between hello packets to 5 seconds, and the time after which a router is considered to be down to 15 seconds, for group number 1 on GigabitEthernet interface 0/0/1:

```
Device(config)# interface GigabitEthernet0/0/1
Device(config-if)# standby 1 ip
Device(config-if)# standby 1 timers 5 15
```

The following shows how to set the time between hello packets to 300 milliseconds, and the time after which a router is considered to be down to 900 milliseconds, for the active hot standby router interface located at 172.19.10.1 on GigabitEthernet interface 0/0/1:

```
Device(config)# interface GigabitEthernet0/0/1
Device(config-if)# standby 1 ip 172.19.10.1
Device(config-if)# standby 1 timers msec 300 msec 900
```

The following shows how to sets the time between hello packets to 15 milliseconds, and the time after which a router is considered to be down to 50 milliseconds, for the active hot standby router interface located at 172.18.10.1 on GigabitEthernet interface 0/0/1. The holdtime is larger than three times the hellotime because the minimum holdtime value in milliseconds is 50:

```
Device(config)# interface GigabitEthernet0/0/1
Device(config-if)# standby 1 ip 172.18.10.1
Device(config-if)# standby 1 timers msec 15 msec 50
```

standby track

To configure Hot Standby Router Protocol (HSRP) to track an object and change the active hot standby or standby router priority on the basis of the state of the object, use the **standby track** command in interface configuration mode. To remove tracking, use the **no** form of this command.

standby *group-number* **track** { *object-number* | **range** *object-number* | [**decrement** *priority-decrement*] } [**shutdown**]
no standby *group-number* **track** *object-number*

Syntax Description

object-number	Object number that represents the object to be tracked. The range is from 1 to 1000. The default is 1.
range *object-number*	Specifies the range of object number that represents the object to be tracked. The range is from 1 to 1000.
decrement *priority-decrement*	(Optional) Specifies the amount by which the Hot Standby priority for the router is decremented (or incremented) when the tracked object goes down (or comes back up). The range is from 1 to 255. The default is 10.
shutdown	(Optional) Changes the HSRP group to the initState method on the basis of the state of a tracked object.

Command Default

There is no tracking.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE standby <*group-number*> track command.

Examples

The following example shows how the tracking process is configured to track the IP-routing capability of serial interface 1/0. HSRP on GigabitEthernet interface 0/0/1 then registers with the tracking process to be informed of any changes to the IP-routing state of the serial interface 1/0. If the IP state on the serial interface 1/0 goes down, the priority of the HSRP group is reduced by 10.

If both the serial interfaces are operational, Router A will be the HSRP active router because it has the higher priority. However, if IP routing on the serial interface 1/0 in Router A fails, the HSRP group priority will be reduced and the Router B will take over as the active router, thus maintaining a default virtual gateway service to the hosts on the 10.1.0.0 subnet.

For backward compatibility of Cisco Catalyst SD-WAN Manager Release 20.15.4 with devices running Cisco IOS XE Catalyst SD-WAN Release 17.15.3 or earlier, when using CLI device templates or CLI add on feature templates, use a different form of **standby track** command.

If **standby** *group-number* **track** *object-number* **decrement** *priority-decrement* configured, use **standby** *group-number* **track** *object-number* **decrement-deprecated** *priority-decrement*instead. For example, if you use standby 1 track 100 decrement 20, configure the following command:

```
standby 1 track 100 decrement-deprecated 20
```

For **standby** *group-number* **track** *object-number* **shutdown** configured, use **standby** *group-number* **track** *object-number* **shutdown-deprecated** instead. For example, if you use standby 1 track 101 shutdown, configure the following command:

```
standby 1 track 101 shutdown-deprecated
```

Device A Configuration

```
Device(config)# track 100 interface serial1/0 ip routing
Device(config-track)# exit
Device(config)# interface GigabitEthernet0/0/1
Device(config-if)# ip address 10.1.0.21 255.255.0.0
Device(config-if)# standby 1 ip 10.1.0.1
Device(config-if)# standby 1 preempt
Device(config-if)# standby 1 priority 105
Device(config-if)# standby 1 track 100 decrement 10
```

Device B Configuration

```
Device(config)# track 100 interface serial1/0 ip routing
Device(config-track)# exit
Device(config)# interface GigabitEthernet0/0/1
```

```
Device(config-if)# ip address 10.1.0.22 255.255.0.0
Device(config-if)# standby 1 ip 10.1.0.1
Device(config-if)# standby 1 preempt
Device(config-if)# standby 1 priority 11
Device(config-if)# standby 1 track 100 decrement 10
```

The following example shows how to change the configuration of a tracked object to include the HSRP Group Shutdown feature:

```
Device(config-if)# no standby 1 track 101 decrement 10
Device(config-if)# standby 1 track 101 shutdown
```

standby version

To change the version of the Hot Standby Router Protocol (HSRP), use the **standby version** command in interface configuration mode. To set the HSRP version to the default version (version 1), use the **no** form of this command.

standby version { **1** | **2** }
no standby version

Syntax Description

1	Specifies HSRP version 1.
2	Specifies HSRP version 2.

Command Default

HSRP version 1 is the default HSRP version.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

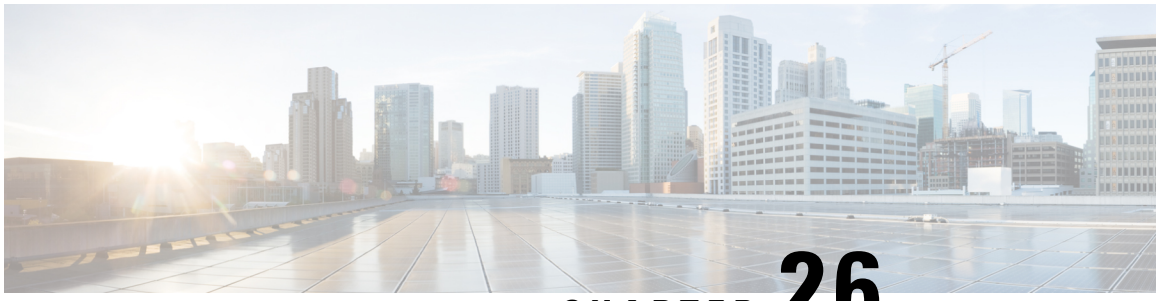
For usage guidelines, see the Cisco IOS XE standby <*group-number*> version command.

The **no standby** or **no standby version** commands resets the version to 1. If standby IPv6 groups are present on the interface, then the **no standby** command is rejected because v6 groups are not supported with version 1.

Examples

The following example shows how to configure HSRP version 2 on an GigabitEthernet interface 0/0/1 with a group number of 500:

```
Device(config)# interface GigabitEthernet 0/0/1
Device(config-if)# standby version 2
Device(config-if)# standby 500 ip 172.20.100.10
Device(config-if)# standby 500 priority 110
Device(config-if)# standby 500 preempt
Device(config-if)# standby 500 timers 5 15
```



CHAPTER 26

Ignition Power Management Commands

•
• ignition enable, on page 303
• ignition sense, on page 304
• ignition battery-type, on page 305
• ignition off-timer, on page 305
• ignition undervoltage threshold, on page 306
• ignition sense-voltage threshold, on page 307
• ignition sense-voltage on-threshold off-threshold, on page 307

ignition enable

To enable the ignition module in the Cisco IR1800 routers, use the **ignition enable** command in global configuration mode.

To disable ignition power management, configure **no ignition enable** and **no ignition sense**.

ignition enable

no ignition enable

Syntax Description

Syntax	Description
ignition	Configure ignition power management on the router.
enable	Enable ignition power management on the router.

Command Default

No default behavior or values.

Command Modes

None.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	This command was introduced.

Usage Guidelines None

Example

The following example configures the router to detect whether a vehicle ignition is on or off:

```
ignition enable
ignition sense
```

ignition sense

To detect whether the ignition is on/off, use the **ignition sense** command in global configuration mode.

To disable ignition sense, configure **no ignition sense**.



Note The **no ignition sense** command is applicable only for IR1835 devices.

ignition sense

no ignition sense

Syntax Description

Syntax	Description
ignition sense	Configure the router to monitor the power supply voltage and detect whether ignition is on or off based on the configured thresholds. **Note** When ignition sense is disabled (on IR1835 only), it uses the ignition signal pin to detect whether ignition is on or off.

Command Default No default behavior or values.

Command Modes None.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	This command was introduced.

Usage Guidelines None.

Example

The following example configures the router to detect whether a vehicle ignition is on or off:

```
ignition enable
ignition sense
```

ignition battery-type

To configure the battery type used for input voltage, use the **ignition battery-type** command in global configuration mode.

ignition *battery-type* { **12 24** }

Syntax Description

Syntax	Description
battery-type	Configures the battery type as 12 V or 24 V.

Command Default

The default battery type is 12 V.

Command Modes

None.

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	This command was introduced.

Usage Guidelines

None.

Example

The following example shows the battery type being configured as 12 volts:

```
ignition battery-type 12v
```

ignition off-timer

To delay router shutdown after the ignition status changes to **off**, use the **ignition off-timer command** in global configuration mode.

ignition off-timer *seconds*

Syntax Description

Syntax	Description
off-timer	Configures a delay (in seconds) before the router shuts down after the ignition is turned off.

Note The device shutdown process begins approximately 100 seconds before the configured off-timer value.

Command Default 300 seconds.

Command Modes None.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	This command was introduced.

Usage Guidelines None.

Example

The following example configures a delay of 300 seconds before the router shuts down after the ignition is turned off:

```
ignition off-timer 300
```

ignition undervoltage threshold

To configure undervoltage parameter to trigger system shutdown if the voltage drops below a specific threshold, use the **ignition undervoltage threshold** command in global configuration mode.

ignition undervoltage threshold *volts millivolts*

Syntax Description

Syntax	Description
undervoltage threshold	Configures the undervoltage parameter to trigger system shutdown if the voltage drops below a specific threshold.

Command Default 9.000 V

Command Modes None.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	This command was introduced.

Usage Guidelines None

Example

The following example configures an undervoltage of 9 V (shown as 9 V and 0 millivolts):

```
ignition undervoltage threshold 9 0
```

ignition sense-voltage threshold

To configure only a single threshold and set the **on-threshold** to threshold +0.2V and the **off-threshold** to threshold -0.2V, use the **ignition sense-voltage threshold** command in global configuration mode.

ignition sense-voltage threshold

Syntax Description

Syntax	Description
sense-voltage threshold	Configures only a single threshold and sets the on-threshold to threshold+0.2V and the off-threshold to threshold-0.2V

Command Default

No default behavior or values.

Command Modes

None.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	This command was introduced.

Usage Guidelines

None

Example

The following example configures an on-threshold voltage of +0.2V, and an off-threshold voltage of -0.2V:

```
ignition sense-voltage threshold
```

ignition sense-voltage on-threshold off-threshold

To configure the on-threshold voltage and off-threshold voltage separately, use the **ignition sense-voltage on-threshold off-threshold** command in global configuration mode.

ignition sense-voltage on-threshold *volts millivolts* **off-threshold** *volts millivolts*

Syntax Description

Syntax	Description
on-threshold	Configures the voltage above which the router will be powered on if it is currently off.
off-threshold	Configures the voltage below which the router will be powered off if it is currently on.

Command Default

No default behavior or values.

Command Modes None.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.18.1a	This command was introduced.

Usage Guidelines None

Example

The following example configures an on-threshold voltage of 11 volts and 900 millivolts, and an off-threshold voltage of 11 volts and 500 millivolts:

```
ignition sense-voltage on-threshold 11 900 off-threshold 11 500
```



CHAPTER 27

Interface Commands

- address (VRRP), on page 310
- channel-group, on page 311
- border, on page 311
- description (interface configuration), on page 312
- duplex, on page 313
- encapsulation, on page 313
- hold-queue, on page 314
- hw-module subslot breakout, on page 315
- interface, on page 316
- interface-pair, on page 320
- interface vlan, on page 322
- ip address, on page 323
- ip address dhcp, on page 324
- ip policy route-map, on page 324
- lacp port-priority, on page 325
- lacp system-priority, on page 326
- load-balancing, on page 327
- mtu, on page 327
- negotiation, on page 328
- Port-channel, on page 328
- port-channel load-balance, on page 329
- port-channel load-balance-hash-algo, on page 330
- port-settings, on page 331
- preempt (VRRP), on page 332
- priority vrrp, on page 333
- shutdown (controller), on page 334
- speed, on page 334
- switchport access vlan, on page 336
- switchport mode, on page 336
- timers advertise VRRP, on page 337
- tunnel destination, on page 338
- tunnel mode, on page 339
- tunnel route-via, on page 340

- tunnel source, on page 340
- track ip route, on page 341
- track, on page 342
- track (VRRP), on page 343
- vrf forwarding, on page 344
- vrrp address-family, on page 345
- vrrpv2, on page 346

address (VRRP)

To specify a primary and secondary IP address for VRRP, use the **address primary** command in VRRP interface configuration mode. To remove the primary and secondary IP addresses, use the **no** form of this command.

address *ip-address* [**primary** | **secondary**]
no address *ip-address* [**primary** | **secondary**]

Syntax Description

ip-address	IP address used as VRRP primary.
[primary | secondary]	(Optional) Specifies the primary or secondary address for the VRRP group.

Command Default

None

Command Modes

VRRP interface configuration (config-if-vrrp)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Use the **address** command to specify a primary and secondary virtual device for VRRP. The primary virtual device sends VRRP advertisements to other VRRP devices in the same group. The advertisements communicate the priority and state of the primary and secondary virtual device. The VRRP advertisements are encapsulated into either IPv4 or IPv6 packets (based on the VRRP group configuration) and sent to the appropriate multicast address assigned to the VRRP group.

Examples

The following example shows how to set the primary IP of VRRP group 3 to 10.50.4.3:

```
Device# config-transaction
Device(config)# int GigabitEthernet0/0/2
Device(config-if)# vrrp 3 address-family ipv4
Device(config-if-vrrp)# address 10.50.4.3 primary
```

Table 19: Related Commands

Commands	Description
vrrp address-family	Creates a VRRP group and enters VRRP configuration mode.

channel-group

To configure the interface in a channel group and set the Link Aggregation Control Protocol (LACP) mode, use the **channel-group** command in the interface configuration mode. To remove the channel-group configuration from the interface, use the **no** form on this command.

channel-group *channel-group-number* **mode** { **auto** | **passive** }

no channel-group

Syntax Description

channel-group-number	Integer that identifies the channel group. The range is from 1 to 128.
mode	Sets the LACP mode.
active	Enables LACP unconditionally.
passive	Enables LACP only when an LACP device is detected. This is the default state.

Command Default

No channel groups are assigned.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

This example shows how to configure an EtherChannel with LACP mode as active.

```
Device# config-transaction
Device(config)# interface GigabitEthernet 0/1/2
Device(config-if)# no ip address
Device(config-if)# channnel-group 1 mode active
```

border

To set the TLOC as a border TLOC, use the **border** command in tunnel interface configuration mode. To unset the TLOC as a border TLOC, use the **no** form of this command.

border

Syntax Description

This command has no keywords or arguments.

Command Default

The default is to have TLOC not set as border TLOC (no border).

Command Modes

Tunnel interface configuration (config-tunnel-interface).

Usage Guidelines

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Examples

The following example shows how to configure a TLOC not set as a Border TLOC:

```
Device# config-transaction
Device(config)# sdwan
Device(config-sdwan)# interface GigabitEthernet0/0/0
Device(config-tunnel-interface)# no border
```

description (interface configuration)

To add a description to an interface configuration, use the **description** command in interface configuration mode. To remove the description, use the **no**form of this command.

description *string*
no description

Syntax Description

string	Comment or a description to help you remember what is attached to this interface. This string is limited to 200 characters.

Command Default

No description is added.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

The **description** command is meant solely as a comment to be put in the configuration to help you remember what certain interfaces are used for. The description appears in the output of the following EXEC commands: **morenvram:startup-config**, **showinterfaces**, and**moresystem:running-config**

Examples

The following example shows how to add a description for an ATM interface:

```
Device(config)# interface ATM 0/3/0

Device(config-if)# description Site1
```

duplex

To configure the duplex operation on an interface, use the **duplex** command in interface configuration mode. To return to the default configuration, use the **no** form of this command.

Supported Parameters

full	Specifies full-duplex operation.
half	Specifies half-duplex operation.
auto	Enables autonegotiation. The interface automatically operates at half-duplex or full-duplex mode depending on environmental factors, such as the type of media and the transmission speeds for the peer routers, hubs, and switches used in the network configuration.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE duplex command.

```
interface {intf-name}
speed {value}
duplex {value}
mtu {value}
switchport mode trunk
switchport trunk allowed vlan {vlans}
switchport trunk native vlan {vlans_id}
no shutdown
```

encapsulation

To set the encapsulation method used by the interface, use the **encapsulation** command in interface configuration mode. To remove the encapsulation, use the **no** form of this command.

encapsulation *encapsulation-type*
no encapsulation *encapsulation-type*

Syntax Description

encapsulation-type	Encapsulation type; one of the following keywords: • **dot1q** *vlan-id* ---Enables IEEE 802.1q encapsulation of traffic on a specified subinterface in VLANs. The *vlan-id* argument is a virtual LAN identifier. • **frame-relay** --Frame Relay (for serial interface). • **ppp** -- PPP (for Dialer interface).

Command Default

NA

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates. The following keywords are qualified: • **dot1q** for GigabitEthernet interface . • **ppp** for Dialer interface.
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Command qualified for use in Cisco vManage CLI templates. The following keywords are qualified: • **encapsulation frame-relay** for serial interface.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE encapsulation command.

Examples

The following example shows how to enable frame-relay encapsulation on Serial interface 0:

```
Device(config)# interface Serial 0
Device(config-if)# encapsulation frame-relay
```

The following example shows how to configure Dialer interface 1 for PPP encapsulation:

```
Device(config)# interface Dialer 1
Device(config-if)# encapsulation ppp
```

hold-queue

To limit the length of the IP output queue on an interface, use the **hold-queue** command in interface configuration mode. To restore the default values, use the **no** form of this command.

hold-queue *length* {**in** | **out**}
no hold-queue *length* {**in** | **out**}

Syntax Description

length	Integer that specifies the maximum number of packets in the queue. The range of valid values is from 0 to 240000.
in	Specifies the input queue. The default is 75 packets. For asynchronous interfaces, the default is 10 packets.
out	Specifies the output queue. The default is 40 packets. For asynchronous interfaces, the default is 10 packets.

Command Default

Input hold-queue limit is 75 packets. Output hold-queue limit is 40 packets. Asynchronous interfaces default is 10 packets.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For the usage guidelines, see hold-queue.

Examples

The following example shows how to set the length of the input queue on a Gigabit Ethernet interface:

```
Device(config)# interface GigabitEthernet 1
Device(config-if)# no hold-queue 100 in
```

The following example shows how to set the length of the output queue on a Gigabit Ethernet interface:

```
Device(config)# interface GigabitEthernet 1
Device(config-if)# no hold-queue 450 out
```

hw-module subslot breakout

To configure a single port to support four 10 Gigabit Ethernet interfaces (called port breakout) on a supported platform, use the **hw-module subslot breakout** command in global configuration mode. To cancel the port breakout, use the **no** form of the command.

hw-module subslot *subslot-number* **breakout** *speed port-id*

no hw-module subslot *subslot-number* **breakout** *speed port-id*

Syntax Description

subslot-number	For the supported routers, the supported subslot is **0/2**.
speed	To configure 10 Gigabit Ethernet, use **10g** for this parameter. To cancel the port breakout and return the port to its default speed, use **10g** for this parameter and include the **no** keyword.
port-id	Possible values: • **native_port_0**: Port 0/2/0 in Bay 2 • **native_port_4**: Port 0/2/4 in Bay 2 • **native_port_8**: Port 0/2/8 in Bay 2 • **all**: All ports in Bay 2.

Command Default

Breakout to 10 Gigabit Ethernet interfaces is not configured.

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.14.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines Cisco 8500-12X4QC platforms have three bays of ports: 0, 1, and 2. By default, the ports of Bays 0 and 1 operate in 10 Gigabit Ethernet mode and the ports of Bay 2 operate in 40 Gigabit Ethernet mode.

You can configure one or more of the Bay 2 ports to operate as four 10 Gigabit Ethernet interfaces. This is called breakout. After you configure a port to provide four 10 Gigabit Ethernet interfaces, use a one-to-four breakout cable to connect four cables to the single port.

When you configure port breakout on a device operating in controller mode, such as in a Cisco Catalyst SD-WAN environment, an additional step is required, using the **no interface** command. This step clears any information about the interfaces that the port or ports may have supported in a previous configuration. Clearing this information ensures that the **show sdwan running-config** command output shows the correct interface information. For details, see the examples.

Example 1

The following configures the 0/2/0 port of Bay 2 to 10 Gigabit Ethernet. The result is four 10 Gigabit Ethernet interfaces:

Te0/2/0, Te0/2/1, Te0/2/2, Te0/2/3

The **no interface** command clears any information about the 40 Gigabit Ethernet interface that port 0/2/0 may have supported in a different configuration.

```
Device(config)#hw-module subslot 0/2 breakout 10g port native_port_0
Device(config)#no interface Fo0/2/0
```

Example 2

The following cancels the port breakout to 10 Gigabit Ethernet interfaces. It returns the 0/2/0 port of Bay 2 to its default 40 Gigabit Ethernet speed. The result is one 40 Gigabit Ethernet interface:

Fo0/2/0

The **no interface** commands clear any information about the four 10 Gigabit Ethernet interfaces that port 0/2/0 may have supported in a different configuration.

```
Device(config)#no hw-module subslot 0/2 breakout 10g port native_port_0
Device(config)#no interface Te0/2/0
Device(config)#no interface Te0/2/1
Device(config)#no interface Te0/2/2
Device(config)#no interface Te0/2/3
```

interface

To configure an interface type and to enter interface configuration mode, use the **interface** command in the global configuration mode.

interface *type* *number* **.** *subinterface-number*

interface *type* *slot* / *subslot* / *port* **.** *subinterface-number* [**point-to-point**]

no interface *type* *number* **.** *subinterface-number*

no interface *type* *slot* / *subslot* / *port* **.** *subinterface-number* [**point-to-point**]

Syntax Description

type	Type of interface to be configured. See the table below.
number	Port, connector, or interface card number. The numbers are assigned at the factory at the time of installation or when added to a system; they can be displayed with the **showinterfaces** command.
slot	Chassis slot number. Refer to the appropriate hardware manual for slot information. For SIPs, refer to the platform-specific SPA hardware installation guide or the corresponding "Identifying Slots and Subslots for SIPs and SPAs" topic in the platform-specific SPA software configuration guide.
/ *subslot*	Secondary slot number on a SIP where a SPA is installed. The slash (/) is required. Refer to the platform-specific SPA hardware installation guide and the corresponding "Specifying the Interface Address on a SPA" topic in the platform-specific SPA software configuration guide for subslot information.
/ *port*	Port or interface number. Theslash(/)is required. Refer to the appropriate hardware manual for port information. For SPAs, refer to the corresponding “Specifying the Interface Address on a SPA” topics in the platform-specific SPA software configuration guide.
. *subinterface-number*	Subinterface number in the range 1 to 4294967293. The number that precedes the period (.) must match the number to which this subinterface belongs.
point-to-point	(Optional) Specifies a point-to-point subinterface.

Command Default

No interface types are configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release Amsterdam 17.2.1v	Commands of the following form were qualified for use in Cisco vManage CLI templates: • **interface ATM 0/3/0** • **interface ATM 0/3/0.1 point-to-point** • **interface Dialer 1** • **interface GigabitEthernet 1** • **interface GigabitEthernet 1.101** • **interface Loopback 100** • **interface Tunnel 10** • **interface VirtualPortGroup 0** • **interface Vlan 1**
Cisco IOS XE Release Amsterdam 17.3.1	Commands of the following form were qualified for use in Cisco vManage CLI templates: • **interface Serial 2/0** • **interface Serial 0/1/0** • **interface Serial 0/1/0.2 point-to-point**

Usage Guidelines

The table below displays the keywords that represent the types of interfaces that can be configured with the **interface** command. Replace the *type* argument with the appropriate keyword from the table.

When you want to push a CLI template or add on CLI template after an upgrade, to match the device running configuration, you must come out of the interface configuration. In this case, interface block must end with statement **exit** instead of "!". After configuring the interfaces, before starting on a new feature configuration, exit from the interface configuration mode.

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.15.1a, size limit for interface is within the range 1 to 31 for interface commands.

Usage Guidelines

Table 20: Interface Type Keywords

Keyword	Interface Type
ATM	ATM interface.
Dialer	Dialer interface.
GigabitEthernet	1000-Mbps Ethernet interface.

Keyword	Interface Type
Loopback	Software-only loopback interface that emulates an interface that is always up. It is a virtual interface supported on all platforms. The *number* argument is the number of the loopback interface that you want to create or configure. There is no limit on the number of loopback interfaces that you can create.
Serial	Serial interface.
Tunnel	Tunnel interface; a virtual interface. The *number* argument is the number of the tunnel interface that you want to create or configure. There is no limit on the number of tunnel interfaces that you can create.
Vlan	VLAN interface.
VirtualPortGroup	Virtual Port Group interface.

For more usage guidelines, see interface.

ATM Interface

```
Device(config)# interface ATM 0/3/0
Device(config-if)#
```

```
Device(config)# interface ATM 0/3/0.1 point-to-point
Device(config-if)#
```

Dialer Interface

```
Device(config)# interface Dialer 1
Device(config-if)#
```

GigabitEthernet Interface

```
Device(config)# interface GigabitEthernet 1
Device(config-if)#
```

```
Device(config)# interface GigabitEthernet 1.101
Device(config-if)#
```

Loopback Interface

```
Router(config)# interface Loopback 100
Router(config-if)#
```

Serial Interface

```
Router(config)# interface Serial 2/0
Router(config-if)#
```

```
Router(config)# interface Serial 0/1/0
Router(config-if)#

Router(config)# interface Serial 0/1/0.2 point-to-point
Router(config-if)#

Router(config)# interface Serial 0/0/1:5
Router(config-if)#
```

Tunnel Interface

```
Router(config)# interface Tunnel 10
Router(config-if)#
```

Virtual Port Group Interface

```
Router(config)# interface VirtualPortGroup 0
Router(config-if)#
```

VLAN Interface

```
Router(config)# interface Vlan 1
Router(config-if)#
```

interface-pair

To define two tunnel interfaces for a high availability (HA) configuration, use the **interface-pair** command in ha-pairs mode. To clear the configured tunnels, use the **no** form of this command.

interface-pair *tunnel1* [**active-interface-weight** *active-weight*] *tunnel2* [**backup-interface-weight** *backup-weight*]

no interface-pair

Supported Parameters

tunnel1	Primary tunnel interface for Cisco Umbrella Secure Internet Gateway (SIG).

active-interface-weight *active-weight*	(Optional) Weight value for load balancing. The weight value is applicable in an active-active configuration if multiple HA pairs and tunnels are configured. The weight values of tunnel interfaces determine what portion of traffic each tunnel interface carries. For example, in an active-active configuration configured as follows... • HA pair A: Tunnel01 has a weight value of 10, and Tunnel02 has a weight value of 10. • HA pair B: Tunnel03 has a weight value of 20, and Tunnel04 has a weight value of 20. ...Tunnel03 is assigned twice has much traffic as Tunnel01. Range: 1 to 255 Default: 1
tunnel2	Secondary (backup) tunnel interface for Cisco Umbrella SIG.
backup-interface-weight *backup-weight*	(Optional) Weight value for load balancing. The weight value is applicable in an active-active configuration if multiple HA pairs and tunnels are configured. The weight values of tunnel interfaces determine what portion of traffic each tunnel interface carries. For example, in an active-active configuration configured as follows... • HA pair A: Tunnel01 has a weight value of 10, and Tunnel02 has a weight value of 10. • HA pair B: Tunnel03 has a weight value of 20, and Tunnel04 has a weight value of 20. ...Tunnel03 is assigned twice has much traffic as Tunnel01. Range: 1 to 255 Default: 1

Command Modes

ha-pairs (config-ha-pairs)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

This command is relevant for tunnel interfaces used with Cisco Umbrella SIG tunnels. The tunnel interfaces must meet the following requirements:

- The tunnels must be IPSec or GRE.
- The tunnels must be configured for auto tunnel or manual tunnel to Umbrella or ZScaler as the SIG service provider.

Examples

In the following example, two times as many traffic flows are forwarded to Tunnel100103 (weight configured as 200) as compared with Tunnel100101 (weight configured as 100).

```
Device(config)# sdwan service sig vrf 1
Device(config-vrf-1)# ha-pairs
Device(config-ha-pairs)# interface-pair Tunnel100101 active-interface-weight 100 Tunnel100102
 backup-interface-weight 200
Device(config-ha-pairs)# interface-pair Tunnel100103 active-interface-weight 200 Tunnel100104
 backup-interface-weight 200
```

interface vlan

To create or access a 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*

Syntax Description

vlan-id	VLAN number. The range is 1 to 4094.

Command Default

None.

Command Modes

Global configuration (config)

Usage Guidelines

SVIs are created the first time you enter the **interface Vlan** *vlan-id* command for a particular VLAN. The *vlan-id* corresponds to the VLAN-tag associated with data frames on an IEEE 802.1Q encapsulated trunk or the VLAN ID configured for an access port.

Note When you create an SVI, it does not become active until it is associated with a physical port.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	This command was introduced.

Examples

The following example shows how to configure VLAN 10 and interface Vlan 10 with the IP address 10.0.10.1/24:

```
Device(config)# vlan 10
Device(config-vlan)# exit
Device(config)# interface Vlan 10
Device(config-Vlan-10)# ip address 10.0.10.1 255.255.255.0
Device(config-Vlan-10)#
```

Related Commands

Command	Description
show interfaces	Displays the administrative and operational status of all interfaces or a specified interface.

ip address

To set a primary or secondary IP address for an interface, use the **ip address** command in interface or sub-interface configuration mode. To remove an IP address or disable IP processing, use the **no** form of this command.

ip address *ip-address* [*mask*]
no ip address [*ip-address*] [*mask*]

Syntax Description

ip-address	IP address.
mask	(Optional) Mask for the associated IP subnet.

Command Default

No IP address is defined for the interface.

Command Modes

Interface configuration (config-if)

Sub-interface configuration (config-subif)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For the usage guidelines, see the Cisco IOS XE ip address command.

Examples

```
Device(config)# interface ATM 0/3/0.1 point-to-point

Device(config-if)# ip address 192.10.6.5
Device(config)# interface ATM 0/3/0.1

Device(config-subif)# ip address 10.0.0.0 255.255.255.252
Device(config)# interface Serial 0/1/0.2

Device(config-if)# ip address 10.1.1.1 255.255.255.0
Device(config)# interface Serial 0/0/1:5

Device(config-if)# ip address 10.1.1.1 255.255.255.0
Device(config)# interface MFR1

Device(config-if)# ip address 10.4.4.4 255.255.255.0
```

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

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.

Command Default

The client identifier is an ASCII value.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For the usage guidelines, see ip address dhcp.

Examples

```
Device(config)# interface GigabitEthernet 1

Device(config-if)# ip address dhcp client-id GigabitEthernet 1
```

ip policy route-map

To identify a route map to use for policy routing on an interface, use the **ip policy route-map** command in interface configuration mode. To disable policy routing on the interface, use the **no**form of this command.

ip policy route-map *map-tag*
no ip policy route-map

Syntax Description

map-tag	Name of the route map to use for policy routing. The name must match a *map-tag* value specified by a **route-map** command.

Command Default

No policy routing occurs on the interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

You might enable policy routing if you want your packets to take a route other than the obvious shortest path.

For usage guidelines, see the Cisco IOS XE ip policy route-map command.

Examples

The following example sends packets with the destination IP address of 172.21.16.18 to a router at IP address 172.30.3.20:

```
interface serial 0
 ip policy route-map wethersfield
!
route-map wethersfield
 match ip address 172.21.16.18
 set ip next-hop 172.30.3.20
```

```
Device(config)# interface GigabitEthernet 1.101
Device(config-if)# ip nbar protocol-discovery
Device(config-if)# ip policy route-map policy1
```

lacp port-priority

To set the LACP priority for a physical interface, use the **lacp port-priority** command in the interface configuration mode. To return to the default setting, use the **no** form on this command.

lacp port-priority *priority*

no lacp port-priority

Syntax Description

priority	Integer that indicates the priority for the physical interface. The range is from 0 to 65535. The default is 32768.

Command Default

The default system priority is set to 32768.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

You may assign a port priority to each port on a device running LACP. You can specify the port priority by using the lacp port-priority command or use the default port priority (32768). The port priority is used to decide which ports should be put in standby mode when a hardware limitation or the lacp max-bundle command

configuration prevents all compatible ports from aggregating. Priority is supported only on port channels with LACP-enabled physical interfaces.

Note A high priority number means a low priority.

To verify the configured port priority, use the show lacp internal command.

The following example shows how to set a port priority of 23700 for an interface:

```
Device# config-transaction
Device(config)# interface GigabitEthernet 0/1/2
Device(config-if)# lacp port-priority 23700
```

lacp system-priority

To set the LACP priority for a system, use the **lacp system-priority** command in the global configuration mode. To return to the default setting, use the **no** form on this command.

lacp system-priority *priority*

no lacp system-priority

Syntax Description

priority	Integer that indicates the LACP priority for the system. The range is from 0 to 65535. The default is 32768.

Command Default

The default system priority is set to 32768.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

You can assign a system priority to each device running LACP. You can specify the system priority by using the lacp system-priority command or use the default system priority (32768). The system priority is used with the MAC address of the device to form the system ID and is used during negotiation with the other systems. The system priority is supported only on port channels with LACP-enabled physical interfaces.

Note A high priority number means a low priority.

To verify the configured system priority, issue the show lacp command.

The following example shows how to set a system priority of 25500 for a device:

```
Device# config-transaction
Device(config)# lacp system-priority 25500
```

load-balancing

To apply a load-balancing method to a Gigabit EtherChannel (GEC) interface, use the **load-balancing** command in the interface configuration mode. To reset to the default, use the **no** form on this command.

load-balancing { **flow** | **vlan** }

no load-balancing

Command Default

The port channel uses the global load-balancing configuration.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For more information about this command, see Cisco IOS XE load-balancingcommand.

This example shows how to set the load-balancing method to VLAN-manual.

```
Device# config-transaction
Device(config)# interface port-channel 1
Device(config-if)# load-balancing vlan
```

mtu

To adjust the maximum packet size or maximum transmission unit (MTU) size, use the **mtu** command in interface configuration mode. To restore the MTU value to its original default value, use the **no** form of this command.

mtu *bytes*
no mtu

Syntax Description

bytes	MTU size, in bytes.

Command Default

The default MTU size for GigabitEthernet interface is 1500 bytes.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For the usage guidelines, see mtu.

Examples

```
Device(config)# interface GigabitEthernet 1
Device(config-if)# mtu 1000
```

negotiation

To enable advertisement of speed, duplex mode, and flow control on a Gigabit Ethernet interface, use the **negotiation** command in interface configuration mode. To disable automatic negotiation, use the **no** form of this command.

negotiation auto
no negotiation [**auto**]

Syntax Description

auto	Specifies enabling the autonegotiation protocol to configure the speed, duplex, and automatic flow control of the Gigabit Ethernet interface. By default, this is set.

Command Default

Autonegotiation is enabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE negotiation command.

Examples

```
Device(config)# interface GigabitEthernet 1
Device(config-if)# negotiation auto
```

Port-channel

To create a port-channel virtual interface, use the **Port-channel** command in the global configuration mode. To remove a port-channel, use the **no** form on this command.

Port-channel *channel-number*

no Port-channel

Syntax Description

channel-number	Channel number assigned to this port-channel interface.

Command Default There are no default values.

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

In the following example how to create a port-channel interface.

```
Device# config-transaction
Device(config)# interface Port-channel 1
Device(config-if)# ip address 10.0.0.1 255.255.255.0
```

port-channel load-balance

To set the load-distribution method among the ports in the EtherChannel, use the **port-channel load-balance** command in the global configuration mode. To reset the load-balancing function to the default setting, use the **no** form of this command, use the **no** form on this command.

port-channel load-balance

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.
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-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.

Command Default The default is src-dst-ip.

Command Modes Global configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

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.

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

```
Device# config-transaction
Device(config)# port-channel load-balance dst-mac
```

port-channel load-balance-hash-algo

To enable load balancing for the EtherChannel, use the **port-channel load-balance-hash-algo** command in the global configuration mode. To reset the load balancing to the default setting, use the **no** form of this command.

port-channel load-balance-hash-algo

no port-channel load-balance-hash-algo

Syntax Description

dst-ip	Specifies load balancing based on the destination host IP address.
dst-mac	Specifies load balancing 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.
sdwan	Enables load balancing on the transport side of Cisco IOS XE Catalyst SD-WAN devices.
src-dst-ip	Specifies load balancing based on the source and destination host IP address.
src-dst-mac	Specifies load balancing based on the source and destination host MAC address.
src-ip	Specifies load balancing based on the source host IP address.
src-mac	Specifies load balancing 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.

Command Default

The default is src-dst-ip.

Command Modes

Global configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.14.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

This example shows how to enable load balancing and apply the desired hash algorithm for traffic distribution on the transport side of Cisco IOS XE Catalyst SD-WAN devices.

Example 1: The following example displays the output for load balancing IPv4 traffic with the default hash algorithm, **src-dst-ip**, applied. Other hash algorithms, such as **ip-and-ports** or **src-ip-only**, can also be applied.

```
Device(config)#port-channel load-balance-hash-algo sdwan
Device(config)#sdwan
Device(config-sdwan)#ip load-sharing algorithm src-dst-ip
```

Example 2: The following example displays the output for load balancing IPv6 traffic with the hash algorithm, **ip-and-ports**, applied. Other hash algorithms, such as **src-dst-ip** or **src-ip-only**, can also be applied.

```
Device(config)#port-channel load-balance-hash-algo sdwan
Device(config)#sdwan
Device(config-sdwan)#ipv6 load-sharing algorithm ip-and-ports
```

port-settings

To configure supported speed, duplex mode, and auto-negotiation settings in one interface configuration request, use the **port-settings** command in interface configuration mode. To reset only the parameters that you specify, use the **no** or **default** form of this command.

port-settings [**speed** *speed-value* | **speed auto-list** *speed-values*] [**duplex** { **auto** | **full** | **half** }] [**autoneg** { **enable** | **disable** }]
no port-settings [**speed** [*speed-value* | **auto-list** *speed-values*]] [**duplex** [**auto** | **full** | **half**]] [**autoneg** [**enable** | **disable**]]
default port-settings [**speed**] [**duplex**] [**autoneg**]

Syntax Description

speed *speed-value*	Configures a supported fixed interface speed. Available values depend on the platform and interface type.
speed auto-list *speed-values*	Configures the supported speeds that the interface advertises during auto-negotiation.
duplex auto	Enables automatic duplex selection on supported interfaces.
duplex full	Configures full-duplex operation.
duplex half	Configures half-duplex operation.
autoneg enable	Enables auto-negotiation.
autoneg disable	Disables auto-negotiation.

Command Default

Default speed, duplex, and auto-negotiation behavior depends on the platform, interface type, mode, module, and media.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 26.2.1	Command introduced.

Usage Guidelines

You can include one, two, or all three parameters. A parameter that you omit retains its existing configured value. Specify parameters in the order **speed**, **duplex**, and **autoneg**.

The **no** and **default** forms reset only the parameters that you specify. Normal **show running-config** output displays the equivalent legacy commands; **show running-config yang** displays **port-settings**.

Use a GigabitEthernet RJ45 interface for speed, duplex, and auto-negotiation examples. SFP and SFP+ interfaces do not support these settings.



Note The new **port-settings** values are stored in CDB. Legacy speed, duplex, and auto-negotiation nodes are virtual compatibility nodes, so a direct **confd_cmd get** for a legacy node can fail with `Not a CDB path`; this is expected. If a **port-settings** leaf is not explicitly stored, **confd_cmd get** can return `item does not exist`, which can represent a default or unconfigured value.

Examples

The following example configures 100 Mbps, half duplex, and disables auto-negotiation on a GigabitEthernet RJ45 interface.

```
Device# configure terminal
Device(config)# interface GigabitEthernet0/1/7
Device(config-if)# port-settings speed 100 duplex half autoneg disable
```

The following example resets only the duplex parameter to its default.

```
Device(config-if)# default port-settings duplex
```

preempt (VRRP)

VRRP preempt is enabled by default. This means, a VRRP router with higher priority than the primary VRRP router will take over as primary router. To delay preemption, so that the higher priority router waits for a minimum period of time before taking over, use the **preempt delay minimum** command. To restore the default behavior (preempt with no delay), use the **no** form of the command.

preempt delay minimum *seconds*
no preempt delay minimum *seconds*

Syntax Description

seconds Minimum number of seconds the router waits before issuing an advertisement claiming virtual IP address ownership to be the primary router.

- The router that is IP address owner preempts the delay of the higher authority router, regardless of the setting of this command.
- The range is 1 to 3600 seconds (1 hour).

Command Default

VRRP preempt is enabled.

seconds : 0 (no delay)

Command Modes

VRRP configuration mode (config-if-vrrp)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

By default, the router being configured with this command takes over as primary router for the virtual router if it has a higher priority than the current primary router. You can configure a minimum delay, which causes the VRRP router to wait for the specified number of seconds before issuing an advertisement claiming virtual IP address ownership to be the primary router.

Examples

```
Device# configure terminal
Device(config)# interface GigabitEthernet 0/0/1
Device(config-if)# ip address 172.16.6.5 255.255.255.0
Device(config-if)# vrrp 10 address-family ipv4 description working-group
Device(config-if-vrrp)# preempt delay minimum 380
Device(config-if-vrrp)# priority 200
```

priority vrrp

To set the priority for the Virtual Router Redundancy Protocol (VRRP), use the **priority** command. To revert to the default value, use the **no** form of this command.

priority *level*
no priority

Syntax Description

level	Interface priority for a virtual router. The range of values is from 1 to 254. If this router is the owner of the IP addresses, then the value is automatically set to 254. The default is 100.

Command Default

The default value is 100. For switches whose interface IP address is the same as the primary virtual IP address, the default value is 254.

Command Modes

VRRP configuration mode (config-if-vrrp)

Command History

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

The priority determines whether or not a VRRP router functions as a virtual router backup, the order of ascendancy for the VRRP router to become a virtual router master if the virtual router master fails, the role that each VRRP router plays, and what happens if the virtual router master fails.

If a VRRP router owns the IP address of the virtual router and the IP address of the physical interface, then this router functions as a virtual router master.

By default, a preemptive scheme is enabled. A backup high-priority virtual router that becomes available takes over for the backup virtual router that was elected to become the virtual router master. If you disable preemption, then the backup virtual router that is elected to become the virtual router master remains the master until the original virtual router master recovers and becomes the master again.

This command does not require a license.

Examples

```
Device(config)# interface GigabitEthernet 1
Device(config-if)# vrrp 64 address-family ipv4
Device(config-if-vrrp)# priority 11
```

shutdown (controller)

To shut down a DSL group, use the **shutdown** command in controller configuration mode. To reactivate the DSL group, use the **no** form of the command.

shutdown

no shutdown

Syntax Description This command has no arguments or keywords.

Command Default Using this command assumes that the interface is already enabled. By default, if this command is not issued, the interface remains enabled.

Command Modes Controller configuration (config-controller)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Qualified for use in Cisco vManage CLI templates.

Examples

```
Router(config)# controller SHDSL 0/1/0
Router(config-controller)# termination cpe
Router(config-controller)# mode atm
Router(config-controller)# dsl-group 0 pairs 0
Router(config-controller-dsl-group)# shdsl rate auto
...
Router(config-controller-dsl-group)# ignore crc always
Router(config-controller-dsl-group)# shutdown
Router(config-controller-dsl-group)# no shutdown
Router(config-controller-dsl-group)#
```

speed

To set the speed of the interface, use the **speed** command in interface configuration (config-if) mode. To return to the default configuration, use the **no** form of this command.

speed *speed*

no speed [*speed*]

Syntax Description

speed	Interface speed, in Mbps. Values: 10, 100, 1000, 2500, 5000, 10000, auto The auto option negotiates the link speed, according to the speed of the peer device. If the peer is using a fixed speed, then the device uses that fixed speed. If the peer is also using auto negotiation, then the two devices negotiate the highest possible speed, which is dependent on the interface type. Default: auto

Command Default

auto

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For fiber small form-factor pluggable modules (SFPs), the supported speed is 1 Gbps full duplex. For copper SFPs, the supported speeds are 10/100/1000 Mbps and half/full duplex. By default, the router autonegotiates the speed and duplex values for the interfaces.

To use a fixed speed and duplex configuration for interfaces that do not support autonegotiation, disable autonegotiation and then use the speed and duplex commands to set the appropriate interface link characteristics.

The following example configures the speed as 100 Mbps, then displays this value using the **show running interface** command.

```
Device(config)# interface GigabitEthernet1/0/6
Device(config-if)# speed 100
Device(config-if)# commit
Commit complete.
Device(config-if)# end
Device#show running interface gi1/0/6
Building configuration...

Current configuration : 48 bytes
!
interface GigabitEthernet1/0/6
 speed 100
end
```

The following example configures the speed as 100 Mbps, then uses **no speed** to cancel the speed configuration. After canceling the speed configuration, the **show running interface** command shows that no speed is currently configured.

```
Device(config)# interface GigabitEthernet1/0/6
Device(config-if)# speed 100
Device(config-if)# commit
Commit complete.
Device(config-if)# no speed
Device(config-if)# commit
Commit complete.
```

```
Device(config-if)# end
Device#show running interface gi1/0/6
Building configuration...

Current configuration : 38 bytes
!
interface GigabitEthernet1/0/6
end
```

switchport access vlan

To set the VLAN when the interface is in access mode, use the **switchport access vlan** command in interface configuration or template configuration mode. To reset the access-mode VLAN to the appropriate default VLAN for the device, use the **no** form of this command.

Supported Parameters

vlan-id	VLAN to set when the interface is in access mode. Valid values are from 1 to 4094. • 1-2349—VLAN ID Range 1 • 2450-4095—VLAN ID Range 2

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE switchport access vlan command.

Examples

```
interface {intf-name}
switchport mode access
switchport access vlan {vlan_id}
dot1x pae authenticator
authentication order dot1x mab
authentication host-mode single-host
authentication port-control auto
authentication timer reauthenticate <timer_num/server>
authentication timer inactivity <timer_num/server>
authentication event server dead action authorize vlan {critical_vlan}
authentication event fail action authorize vlan {restrict_vlan}
authentication event no-response action authorize vlan {guest_vlan}
no shutdown
```

switchport mode

To set the interface type, use the **switchport mode** command in interface configuration mode. Use the **no** form of this command to reset the mode to the appropriate default mode for the device.

Supported Parameters

access	Sets a nontrunking, nontagged single VLAN Layer 2 interface.
trunk	Specifies a trunking VLAN Layer 2 interface.
native vlan *vlan-id*	The particular native VLAN. Valid values are: 1-2349—VLAN ID Range 1 2450-4095—VLAN ID Range 2
allowed vlan *vlan-list*	Sets the list of allowed VLANs that transmit traffic from this interface in tagged format when in trunking mode.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE switchport mode command.

Examples

```
interface {intf-name}
switchport mode access
switchport access vlan {vlan_id}
dot1x pae authenticator
authentication order dot1x mab
authentication host-mode single-host
authentication port-control auto
authentication timer reauthenticate <timer_num/server>
authentication timer inactivity <timer_num/server>
authentication event server dead action authorize vlan {critical_vlan}
authentication event fail action authorize vlan {restrict_vlan}
authentication event no-response action authorize vlan {guest_vlan}
no shutdown


interface {intf-name}
speed {value}
duplex {value}
mtu {value}
switchport mode trunk
switchport trunk allowed vlan {vlans}
switchport trunk native vlan {vlans_id}
no shutdown
```

timers advertise VRRP

To set the advertisement timer for VRRP, use **timers advertise** command in VRRP interface configuration mode. To remove advertisement timer custom setting, use the **no** form of this command.

timers advertise *interval*
no timers advertise *interval*

Syntax Description

interval	Sets the VRRP advertisement timer in milliseconds.

Command Default

The advertisement timer is set to 1000 milliseconds by default.

Command Modes

VRRP interface configuration (config-if-vrrp)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

The primary virtual device sends VRRP advertisements to other VRRP devices in the same group. The advertisements communicate the priority and state of the primary virtual device. The VRRP advertisements are encapsulated into either IPv4 or IPv6 packets (based on the VRRP group configuration) and sent to the appropriate multicast address assigned to the VRRP group. Use **timers advertise** command to set the advertisement timer for VRRP.

Example

The following example sets VRRP advertisement timer to 1500 milliseconds:

```
SDWAN-Device-01# config-transaction
SDWAN-Device-01(config)# int GigabitEthernet0/0/2
SDWAN-Device-01(config-if)# vrrp 3 address-family ipv4
SDWAN-Device-01(config-if-vrrp)# timers advertise 1500
```

Table 21: Related Commands

Commands	Description
vrrp address-family	Creates a VRRP group and enters VRRP configuration mode.

tunnel destination

To set the destination address for a GRE tunnel interface, use the **tunnel destination** command in interface configuration mode. To remove the destination address, use the **no** form of this command.

tunnel destination *interface-ip-address*
no tunnel destination

Syntax Description

interface-ip-address	IP address of the destination interface.

Command Default

No tunnel interface destination address is set.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For the usage guidelines, see tunnel destination.

The following example shows a GRE tunnel configuration, including tunnel source and destination interfaces specified by IP address:

```
Device(config)# interface Tunnel100512
Device(config-if)# no shutdown
Device(config-if)# vrf forwarding 1
Device(config-if)# ip address 192.168.0.1 255.255.255.248
Device(config-if)# no ip clear-dont-fragment
Device(config-if)# ip tcp adjust-mss 1387
Device(config-if)# ip mtu 1500
Device(config-if)# tunnel source 10.0.3.55
Device(config-if)# tunnel destination 10.0.3.149
```

tunnel mode

To set the encapsulation mode for the tunnel interface, use the **tunnel mode** command in interface configuration mode. To restore the default mode, use the no form of this command.

tunnel mode sdwan
no tunnel mode

Syntax Description

sdwan	Enables SD-WAN tunneling mode.

Command Default

The default is GRE tunneling.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Examples

The following example shows how to enable SD-WAN tunneling mode:

```
Device(config)# interface Tunnel 1
Device(config-if)# tunnel source GigabitEhternet0/2.101
Device(config-if)# tunnel mode sdwan
```

tunnel route-via

To specify the outgoing interface of the tunnel transport, use the **tunnelroute-via** command in interface configuration mode. To disable the source address selection, use the **no** form of this command.

Supported Parameters

interface-type	Indicates the type of interface.
interface-number	Indicates the interface number of the interface configured as the tunnel transport.
mandatory	Drops the traffic if the route is not available.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE tunnel route-via command.

```
interface Tunnel100512
 tunnel route-via GigabitEthernet1 mandatory
ip sdwan route vrf 1 0.0.0.0/0 service sig
sdwan service sig vrf global
 ha-pairs
  interface-pair Tunnel100511 active-interface-weight 100 Tunnel100512 backup-interface-weight
 200
```

tunnel source

To set the source address for a tunnel interface, use the **tunnel source** command in interface configuration mode. To remove the source address, use the **no** form of this command.

tunnel source *interface-type interface-number interface-ip-address*
no tunnel source

Syntax Description

interface-type	Interface type.
interface-number	Port, connector, or interface card number. The numbers are assigned at the factory at the time of installation or when added to a system and can be displayed with the **show interfaces** command.
interface-ip-address	IP address of the source interface.

Command Default

No tunnel interface source address is set.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Added *interface-ip-address* option.

Usage Guidelines

For the usage guidelines, see tunnel source.

The following example shows how to set a Gigabit Ethernet interface as the tunnel source:

```
Device(config)# interface Tunnel 1
Device(config-if)# tunnel source GigabitEthernet0/2.101
Device(config-if)# tunnel mode sdwan
```

The following example shows a GRE tunnel configuration, including tunnel source and destination interfaces specified by IP address:

```
Device(config)# interface Tunnel100512
Device(config-if)# no shutdown
Device(config-if)# vrf forwarding 1
Device(config-if)# ip address 192.168.0.1 255.255.255.248
Device(config-if)# no ip clear-dont-fragment
Device(config-if)# ip tcp adjust-mss 1387
Device(config-if)# ip mtu 1500
Device(config-if)# tunnel source 10.0.3.55
Device(config-if)# tunnel destination 10.0.3.149
```

track ip route

To track the state of an IP route and to enter tracking configuration mode, use the **track ip route** command in global configuration mode. To remove the tracking, use the **no** form of this command.

Supported Parameters

object-number	Object number that represents the object to be tracked. The range is from 1 to 1000.
ip	Tracks an IP route.
ipv6	Tracks an IPv6 route.
address	IP or IPv6 subnet address to the route that is being tracked.
/prefix-length	Number of bits in the address prefix. A forward slash (/) is required.
reachability	Tracks whether the route is reachable.
metric threshold	Tracks the threshold metric. The default up threshold is 254, and the default down threshold is 255.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE track ip route.

Examples

The following example shows how the tracking process is configured to track the reachability of 10.22.0.0/16:

```
Device(config)#  track 1 ip route 10.22.0.0/16 reachability
```

The following example shows how the tracking process is configured to track the threshold metric by using the default threshold metric values:

```
Device(config)#  track 1 ip route 10.22.0.0/16 metric threshold
```

The following example shows how the tracking process is configured to track the threshold metric using the default threshold metric values for an IPv6 route:

```
Device(config)#  track 2 ipv6 route 2001:DB8:0:ABCD::1/10 metric threshold
```

track

To configure an interface or a SIG container list tracking as a single entity, use the **track** command in vrrp configuration mode. To remove the tracking for a list, use the **no** form of this command.

track *track-list-name* [**decrement** *priority*]

Syntax Description

track-list-name	The interface or container list name.
priority	The decrement value for the list priority.

Command Modes

vrrp configuration (config-vrrp)

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Example

The following example shows how to configure a track list for an interface.

```
Device# config terminal
Device (config)# system
Device (config-system)# track-list zs1 interface ge0/1 gre1 ipsec1
Device (config-system-tracker-list-zs1)# exit
```

```
Device (config-system)# exit

Device (config)# vpn 1
Device (config-vpn-1)# name vpn-name
Device (config- vpn-1)# interface ge0/2
Device (config-interface-ge0/2)# ip address 172.16.10.1/24
Device (config-interface-ge0/2)# no shutdown
Device (config-interface-ge0/2)# vrrp 100
Device (config-vrrp-100)# track zs1 decrement 10
Device (config-vrrp-track-zs1)# exit
Device (config-vrrp-100)# ipv4 172.16.10.100
Device (config-vrrp-100)# tloc-change-pref
```

The following example shows how to configure a track list for the SIG container.

```
Device# config terminal
Device (config)# system
Device (config-system)# track-list sig-1 sig-container global
Device (config-system-tracker-list-SIG)# exit
Device (config-system)# exit

Device (config)# vpn 1
Device (config-vpn-1)# name vpn-name
Device (config- vpn-1)# interface ge0/2
Device (config-interface-ge0/2)# ip address 172.16.10.1/24
Device (config-interface-ge0/2)# no shutdown
Device (config-interface-ge0/2)# vrrp 100
Device (config-vrrp-100)# track SIG decrement 10
Device (config-vrrp-track-zs1)# exit
Device (config-vrrp-100)# ipv4 172.16.10.100
Device (config-vrrp-100)# tloc-change-pref
```

track (VRRP)

To enable an object to be tracked using a Virtual Router Redundancy Protocol version 3 (VRRPv3) group, use the **track** command in VRRP configuration mode. To disable the tracking, use the **no** form of this command.

track *object-number* { **shutdown** | [**decrement** *priority*] }
no track *object-number* **shutdown**

Syntax Description

object-number	Object number representing the interface to be tracked. The range is from 1–1000.
shutdown	Shuts down the VRRPv3 group.
decrement *priority*	Sets the priority value by which the VRRP group is reduced if the tracked object state on serial interface VRRPv3 goes down. The valid range is 1–255.

Command Default

Tracking an object using a VRRPv3 group isn't enabled.

Command Modes

VRRP configuration (config-if-vrrp)

Command History

Release	Modification
Cisco IOS XE Release Amsterdam 17.2.1v	Qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For the usage guidelines, see track (VRRP).

Examples

The following example shows how to configure VRRPv3 group shutdown:

```
Device(config)# interface GigabitEthernet1
Device(config-if)# vrrp 2 address-family ipv4
Device(config-if-vrrp)# track 2 shutdown
```

The following example shows how to configure the tracking process to track the state of the IPv6 object using the VRRPv3 group. VRRP on GigabitEthernet interface 0/0/0 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
```

The following example shows how to configure the tracking process to track the state of the IPv4 object. VRRP on GigabitEthernet2 registers with the tracking process to be informed of any changes to the IPv4 object. If the IPv4 object state on interface goes down, then the priority of the VRRP group is reduced by 10:

```
Device(config)# interface GigabitEthernet2
Device(config-if)# ip address 10.10.1.1 255.255.255.0
Device(config-if)# negotiation auto
Device(config-if)# vrrp 1 address-family ipv4
Device(config-if-vrrp)# address 10.10.1.10 primary
Device(config-if-vrrp)# track 400 decrement 10
Device(config-if-vrrp)# tloc-change increase-preference 1
Device(config-if-vrrp)# exit
```

vrf forwarding

To associate a VRF instance or a virtual network with an interface or subinterface, use the **vrf forwarding** command in interface configuration mode. To disassociate a VRF or virtual network from an interface or subinterface, use the **no** form of this command.

vrf forwarding *vrf-name*
no vrf forwarding *vrf-name*

Syntax Description

vrf-name	The VRF name to be associated with the specified interface.

Command Default

The default for an interface is the global routing table.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For the usage guidelines, see vrf forwarding.

Examples

```
Device(config)# interface GigabitEthernet 1
Device(config-if)# vrf forwarding vrf1
```

vrrp address-family

To create a VRRP group and to enter VRRP configuration mode, use the **vrrp address-family** command in interface configuration mode. To remove the VRRP group, use the **no** form of this command.

vrrp *group* **address-family** { **ipv4** | **ipv6** }
no vrrp *group* **address-family** { **ipv4** | **ipv6** }

Syntax Description

group	VRRP group number ranges from 1 to 255.
ipv4	Enter VRRP IPv4 address-family configuration.
ipv6	Enter VRRP IPv6 address-family configuration.

Command Default

None

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Use the **vrrp address-family** command to create a VRRP group and to enter VRRP configuration mode. VRRP is the only FHRP (First Hop Redundancy Protocol) supported by Cisco Catalyst SD-WAN edge routers in controller mode. Once you create the group and specify the address-family, you can configure different settings for VRRP.

Examples

The following example creates and customizes VRRP group 3:

```
Device# config-transaction
Device(config)# int GigabitEthernet0/0/2
Device(config-if)# vrrp 3 address-family ipv4
```

Table 22: Related Commands

Command	Description
address primary (VRRP)	Configures a primary IP address for VRRP.

vrrpv2

To enable the support of VRRP version 2 simultaneously with VRRP version 3, use the **vrrpv2** command in VRRP interface configuration mode. To disable the support of VRRP version 2 group, use the **no** form of this command.

vrrpv2
no vrrpv2

Syntax Description

This command has no keywords or arguments.

Command Default

VRRPv2 is disabled by default.

Command Modes

VRRP interface configuration (config-if-vrrp)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

When you configure VRRP on an interface, the default version is VRRP version 3. When VRRPv3 is in use, VRRPv2 is unavailable. Use **vrrpv2** command to enable support for VRRPv2 simultaneously, to interoperate with devices which only support VRRP version 2.

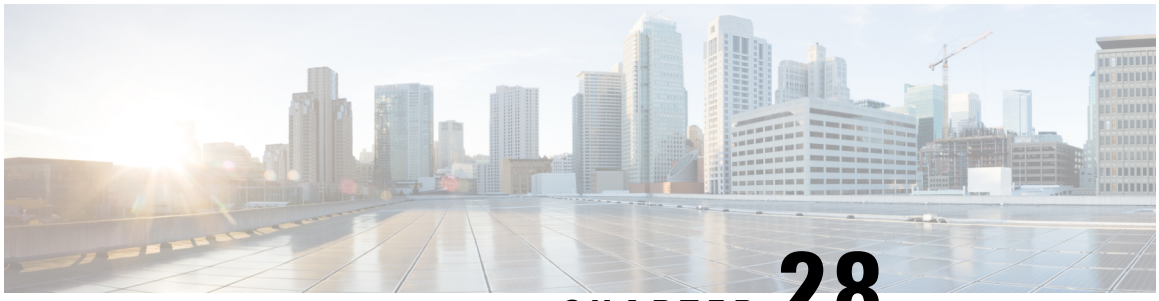
Example

The following example enables the support of VRRPv2 simultaneously with VRRPv3:

```
SDWAN-Device-01# config-transaction
SDWAN-Device-01(config)# int GigabitEthernet0/0/2
SDWAN-Device-01(config-if)# vrrp 3 address-family ipv4
SDWAN-Device-01(config-if-vrrp)# vrrpv2
```

Table 23: Related Commands

Command	Description
vrrp address-family	Creates a VRRP group and enters VRRP configuration mode.



CHAPTER 28

IP Commands

- access-class, on page 349
- address prefix, on page 350
- arp timeout, on page 350
- cdp enable, on page 351
- cdp run, on page 351
- default-router, on page 352
- dns-server, on page 352
- domain-name, on page 353
- ip address, on page 354
- ip address dhcp, on page 355
- ip arp proxy disable, on page 355
- ip bootp server, on page 356
- ip cef load-sharing algorithm, on page 357
- ip-clear-dont-fragment, on page 358
- ip community-list, on page 359
- ip dhcp client vendor-class, on page 361
- ip dhcp conflict logging, on page 362
- ip dhcp use, on page 363
- ip dhcp smart-relay, on page 364
- ip dhcp use hardware-address client-id, on page 365
- ip directed-broadcast, on page 365
- ip dns server, on page 366
- ip domain lookup, on page 367
- ip finger, on page 367
- ip helper-address, on page 368
- ip host, on page 368
- ip host *ip-address*, on page 369
- ip http authentication, on page 370
- ip http client source-interface, on page 371
- ip http secure-server, on page 371
- ip http server, on page 372
- ip http tls-version, on page 373
- ip icmp rate-limit unreachable, on page 373

- ip icmp redirect, on page 374
- ip igmp ssm-map query dns, on page 375
- ip load-sharing algorithm, on page 375
- ip mtu, on page 376
- ip multicast route-limit, on page 377
- ip name-server, on page 378
- ip pim, on page 379
- ip pim bsr-candidate, on page 379
- ip pim rp-address, on page 381
- ip pim rp-candidate, on page 381
- ip prefix-list, on page 383
- ip redirects, on page 383
- ip rcmd, on page 384
- ip rcmd rcp-enable, on page 385
- ip rcmd rsh-enable, on page 386
- ip route vrf, on page 386
- ip route, on page 387
- ip source-route, on page 388
- ip ssh version, on page 389
- ip tcp adjust-mss, on page 390
- ip tcp mss, on page 390
- ip unnumbered, on page 391
- ip virtual-reassembly, on page 391
- ipv6 access-class, on page 392
- ipv6 address, on page 393
- ipv6 address autoconfig, on page 394
- ipv6 address dhcp client request, on page 394
- ipv6 cef load-sharing algorithm, on page 394
- ipv6 dhcp client pd, on page 396
- ipv6 dhcp client vendor-class, on page 396
- ipv6 dhcp pool, on page 397
- ipv6 dhcp relay destination, on page 398
- ipv6 dhcp-relay option vpn, on page 398
- ipv6 dhcp server, on page 399
- ipv6 enable, on page 399
- ipv6 load-sharing algorithm, on page 400
- ipv6 nd other-config-flag, on page 401
- ipv6 nd prefix, on page 401
- ipv6 nd ra suppress, on page 402
- ipv6 nd router-preference, on page 403
- ipv6 redirects, on page 404
- ipv6 route, on page 404
- ipv6-strict-control, on page 405
- ipv6 unnumbered, on page 406
- lease, on page 407
- network (DHCP), on page 407

- option (DHCP), on page 408
- prefix-delegation, on page 409
- prefix-delegation pool, on page 409
- spt-only, on page 409
- vlan internal allocation policy, on page 410
- vendor-specific, on page 411
- vrf (DHCP pool), on page 411

access-class

To restrict incoming and outgoing connections between a particular VTY and the addresses in an access list, use the **access-class** command. To remove access restrictions, use the **no** form of this command.

access-class *access-list-name/number* { **in** | **out** }

no access-class *access-list-name* { **in** | **out** }

Syntax Description

access-list-name/number	You can either enter a name of the access-list or a number. Name of the IPv4 ACL class. The name can be a maximum of 64 alphanumeric characters. The name cannot contain a space or quotation mark. Number of an IP access list. This is a decimal number from 1 to 199 or from 1300 to 2699 .
in	Restricts incoming connections between a particular Cisco device and the addresses in the access list.
out	Restricts outgoing connections between a particular Cisco device and the addresses in the access list.

Command Default

None

Command Modes

Line configuration mode (config-line)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `access-class` command.

Examples

This example shows how to configure an access class on a VTY line:

```
Device (config)# line vty 0 5
Device(config-line)# access-class TEST in
```

address prefix

To specify an address prefix for address assignment, use the **address prefix** command in interface configuration mode. To remove the address prefix, use the **no** form of this command.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE address prefix command.

Examples

The following example shows how to configure a pool called engineering with an IPv6 address prefix:

```
Device(config)# ipv6 dhcp pool engineering
Device(config-dhcpv6)# address prefix 2001:1000::0/64 lifetime infinite
```

arp timeout

To configure how long a dynamically learned IP address and its corresponding Media Control Access (MAC) address remain in the Address Resolution Protocol (ARP) cache, use the **arp timeout** command in interface configuration mode. To restore the default value, use the **no** form of this command.

arp timeout *seconds*
no arp timeout

Syntax Description

seconds	Time (in seconds) that an entry remains in the ARP cache. The general recommended value for ARP timeout is the configured default value, which is 4 hours. If the network has frequent changes to cache entries, change the default to a shorter time period. As you reduce the ARP timeout, your network traffic increases. A low ARP timeout value might lead to network outage, and a value less than an hour (or 3600 seconds) will generate significantly increased traffic across the network. **Caution** We recommend that you set an ARP timeout value greater than 60 seconds.

Command Default

14400 seconds (4 hours)

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

For the usage guidelines, see arp timeout.

Examples

```
Device(config)# interface GigabitEthernet 1
Device(config-if)# arp timeout 7200
```

cdp enable

To enable Cisco Discovery Protocol on an interface, use the **cdp enable** command in interface configuration mode. To disable Cisco Discovery Protocol on an interface, use the **no**form of this command.

cdp enable
no cdp enable

Syntax Description

This command has no arguments or keywords.

Command Default

This command is enabled at the global configuration level and is supported on all interfaces.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For the usage guidelines, see cdp enable.

Examples

```
Device(config)# interface GigabitEthernet 1
Device(config-if)# cdp enable
```

cdp run

To enable Cisco Discovery Protocol, use the **cdp run**command in global configuration mode. To disable Cisco Discovery Protocol, use the **no**form of this command.

cdp run
no cdp run

Syntax Description

This command has no arguments or keywords.

Command Default

This command is enabled on all the platforms.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `cdp run` command.

Examples

In the following example, Cisco Discovery Protocol is enabled globally.

```
Device(config)# cdp run
```

default-router

To specify the default router list for a Dynamic Host Configuration Protocol (DHCP) client, use the **default-router** command in DHCP pool configuration mode. To remove the default router list, use the **no** form of this command.

default-router *address* [*address2* **. . .** *address8*]
no default-router

Syntax Description

address	Specifies the IP address of a router. One IP address is required, although you can specify up to eight addresses in one command line.
address2...address8	(Optional) Specifies up to eight addresses in the command line.

Command Default

No default behavior or values.

Command Modes

DHCP pool configuration (dhcp-config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `default-router` command.

Examples

The following example specifies 10.1.19.15 as the IP address of the default router:

```
Device(config)# ip dhcp pool POOL1
Device(dhcp-config)# default-router 10.1.19.15
```

dns-server

To specify the Domain Name System (DNS) IP servers available to a Dynamic Host Configuration Protocol (DHCP) client, use the **dns-server** command in DHCP pool configuration mode. To remove the DNS server list, use the **no** form of this command.

dns-server *address* [*address2* **. . .** *address8*]
no dns-server

Syntax Description

address	The IP address of a DNS server. One IP address is required, although you can specify up to eight addresses in one command line.
address2...address8	(Optional) Specifies up to eight addresses in the command line. The server addresses should be specified in the order of preference.

Command Default

If DNS IP servers are not configured for a DHCP client, the client cannot correlate host names to IP addresses.

Command Modes

DHCP pool configuration (dhcp-config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

Servers are listed in order of preference (address1 is the most preferred server, address2 is the next most preferred server, and so on).

Examples

The following example specifies 10.12.1.99 as the IP address of the domain name server of the client:

```
Device(config)# ip dhcp pool POOL1
Device(dhcp-config)# dns-server 10.12.1.99
```

domain-name

To specify the default domain for a Domain Name System (DNS) view to use to complete unqualified hostnames (names without a dotted-decimal domain name), use the **domain-name** command in DHCP pool configuration mode. To remove the specification of the default domain name for a DNS view, use the **no** form of this command.

domain-name *domain-name*
no domain-name

Syntax Description

domain-name	Default domain name used to complete unqualified hostnames. **Note** Do not include the initial period that separates an unqualified name from the domain name.

Command Default

No default domain name is defined for the DNS view.

Command Modes

DHCP pool configuration (dhcp-config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `domain name` command.

Examples

The following example shows how to define dns1 as the default DNS view for the DHCP pool named POOL1.

```
Device(config)# ip dhcp pool POOL1
Device(dhcp-config)# domain-name dns1
```

ip address

To set a primary or secondary IP address for an interface, use the **ip address** command in interface or sub-interface configuration mode. To remove an IP address or disable IP processing, use the **no** form of this command.

ip address *ip-address* [*mask*]
no ip address [*ip-address*] [*mask*]

Syntax Description

ip-address	IP address.
mask	(Optional) Mask for the associated IP subnet.

Command Default

No IP address is defined for the interface.

Command Modes

Interface configuration (config-if)

Sub-interface configuration (config-subif)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For the usage guidelines, see the Cisco IOS XE ip address command.

Examples

```
Device(config)# interface ATM 0/3/0.1 point-to-point

Device(config-if)# ip address 192.10.6.5

Device(config)# interface ATM 0/3/0.1

Device(config-subif)# ip address 10.0.0.0 255.255.255.252

Device(config)# interface Serial 0/1/0.2

Device(config-if)# ip address 10.1.1.1 255.255.255.0

Device(config)# interface Serial 0/0/1:5

Device(config-if)# ip address 10.1.1.1 255.255.255.0
```

```
Device(config)# interface MFR1

Device(config-if)# ip address 10.4.4.4 255.255.255.0
```

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

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.

Command Default

The client identifier is an ASCII value.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For the usage guidelines, see ip address dhcp.

Examples

```
Device(config)# interface GigabitEthernet 1

Device(config-if)# ip address dhcp client-id GigabitEthernet 1
```

ip arp proxy disable

To globally disable proxy Address Resolution Protocol (ARP), use the **ip arp proxy disable** command in global configuration mode. To reenable proxy ARP, use the **no** form of this command.

ip arp proxy disable
no ip arp proxy disable

Syntax Description

This command has no arguments or keywords.

Command Default Proxy ARP is enabled.

Command Modes Global configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines The **ip arp proxy disable** command overrides any proxy ARP interface configuration. The **default ip arp proxy** command returns proxy ARP to the default behavior, which is enabled.

Examples The following example disables proxy ARP:

```
Device(config)# ip arp proxy disable
```

The following example enables proxy ARP:

```
Device(config)# no ip arp proxy disable
```

ip bootp server

To enable the Bootstrap Protocol (BOOTP) service on your routing device, use the **ip bootp server** command in global configuration mode. To disable BOOTP services, use the **no** form of the command.

ip bootp server
no ip bootp server

Syntax Description This command has no arguments or keywords.

Command Default Enabled

Command Modes Global configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines For usage guidelines, see the Cisco IOS XE `ip bootp server` command.

Examples In the following example, the BOOTP service is enabled and disabled on the router:

```
Device(config)# ip bootp server
Device(config)# no ip bootp server
```

ip cef load-sharing algorithm

To select a Cisco Express Forwarding load-balancing algorithm for IPv4, 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 { **universal** [*id*] | **include-ports** [**source** [*id*] | **destination** [*id*]] | **src-only** [*id*] }
no ip cef load-sharing algorithm

universal *[id]*	Sets the load-balancing algorithm to the universal algorithm that uses a source and destination IP. (This is set as default).
id	(Optional) Fixed identifier.
include-ports {**source** *[id]* | **destination***[id]*	Sets the load-balancing algorithm to include source port and destination port.
src-only *[id]*	Sets the load-balancing algorithm to include source-only port.

Command Default

The universal load-balancing algorithm is selected. 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 Catalyst SD-WAN Release 17.6.1a	This command was introduced.
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	This command was modified. The **src-only** algorithm is added.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE ip cef load-sharing algorithm command.

You can enable **ECMP keying** to send the configurations for both IPv4 and IPv6.

Examples

The following example shows how to enable the CEF load-balancing algorithm for universal:

```
Device# config-transaction
Device(config)# ip cef load-sharing algorithm universal
```

The following example shows how to enable the IP CEF load-sharing algorithm to include source and destination ports algorithm:

```
Device# config-transaction
Device(config)# ip cef load-sharing algorithm include-ports source destination
Device(config)# commit
```

The following example shows how to enable CEF load-sharing algorithm to src-only port algorithm:

```
Device# config-transaction
Device(config)# ip cef load-sharing algorithm src-only [id]
Device(config)# commit
```

ip-clear-dont-fragment

ip clear-dont-fragment—Clear the Don't Fragment (DF) bit in the IPv4 packet header for packets being transmitted out the interface. When the DF bit is cleared, packets larger than that interface's MTU are fragmented before being sent.

Note **ip clear-dont-fragment** clears the DF bit when there is fragmentation needed and the DF bit is set. For packets not requiring fragmentation, the DF bit is not affected.

The option to clear the Dont Fragment bit is available for Cisco SD-WAN tunnels interfaces only.

By default, the clearing of the DF bit is disabled.

vManage Feature Template

Configuration ► Templates ► Cellular Interface

Configuration ► Templates ► VPN Ethernet Interface

Configuration ► Templates ► VPN Interface DSL IPoE

Configuration ► Templates ► VPN Interface DSL PPPoA

Configuration ► Templates ► VPN Interface DSL PPPoE

Configuration ► Templates ► VPN Interface Multilink

Configuration ► Templates ► VPN Interface T1/E1

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

For more information about this command, see the Cisco IOS XE clear-dont-fragment

Example

This example shows how to clear the DF bit in IPv4 packets being sent out an interface:

```
Device# config-transaction
Device(config)#interface Tunnel 1
Device(config-if)#ip unnumbered GigabitEthernet1
Device(config-if)#ip clear-dont-fragment
Device(config-if)#
```

ip community-list

To create a community list that you can use in a route map to filter BGP routes based on community values, use the **ip community-list** command in global configuration mode. It supports two types of community lists: **standard** and **expanded**.

Standard community list performs an exact match against the specified community values, while the expanded community list uses a regular expression to match community values.

To remove the community-list configuration, use the **no** form of this command.

ip { **community-list** | **community-list-deprecated** } { *standard-list-number* | **standard** *list-name* { **deny** | **permit** | **deny-v1 deny-list** | **permit-v1 permit-list** } [*community-number*] [*AA:NN*] [**internet**] [**local-AS**] [**no-advertise**] [**no-export**] [**gshut**] }

ip { **community-list** | **community-list-deprecated** } { *expanded-list-number* | **expanded** *list-name* { **deny** | **permit** | **deny-v1 deny-list** | **permit-v1 permit-list** } *regular-expression* }

no ip community-list { *standard-list-number* | **standard** *list-name* { **deny** | **permit** } [*community-number*] [*AA:NN*] [**internet**] [**local-AS**] [**no-advertise**] [**no-export**] }

community-list-deprecated	This keyword is provided for backward compatibility. Use this keyword instead of **community-list** if you are using Cisco Catalyst SD-WAN Manager Release 20.15.5 and later with Cisco IOS XE Catalyst SD-WAN devices running 17.14 or earlier.
standard-list-number	Standard community list defined with a number. Range: 1 to 99
standard *list-name*	Standard community list defined with a name.
deny	Exclude routes that match the BGP community attributes specified in this command.
permit	Include routes that match the BGP community attributes specified in this command.
deny-v1 deny-list	These keywords are provided for backward compatibility. Use these keywords instead of **deny** if you are using Cisco Catalyst SD-WAN Manager Release 20.15.1 to 20.15.4 with Cisco IOS XE Catalyst SD-WAN devices running 17.14.x or earlier.
permit-v1 permit-list	These keywords are provided for backward compatibility. Use these keywords instead of **permit** if you are using Cisco Catalyst SD-WAN Manager Release 20.15.1 to 20.15.4 with Cisco IOS XE Catalyst SD-WAN devices running 17.14.x or earlier.

community-number	Community value attached to a BGP route. It is used as a matching criterion to identify specific BGP routes that carry that particular tag, allowing you to either include or exclude those routes in a route map. Range: 1 to 4,294,967,200 A well-known community in a community list is a predefined community value used to tag routes with specific routing policies. Standard type is used to specify these well-known communities or community numbers.
AA:NN	Community value expressed in new format (Autonomous system:community number). Range: 1 to 65535:1 to 65535
internet **local-AS** **no-advertise** **no-export** **gshut**	A well-known community is a predefined community attribute used to tag routes with specific routing policies. • internet: Advertises the route to the internet community. • local-AS: Prevents the advertisement of a route outside local autonomous system • no-advertise: Prevents the advertisement of a route to any BGP peer. • no-export: Prevents the route from being advertised to external BGP peers. • gshut: Community of routes gracefully shut down.
expanded-list-number	Expanded community list defined with a number. Range: 100 to 500
expanded *list-name*	Expanded community list defined with a name.
regular-expression	Regex pattern used to match community values for flexible and complex filtering. Regular expressions are only supported with expanded community lists.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.15.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Route maps use community lists to match BGP community values to control route acceptance, preference, distribution, or advertisement.

If you are using Cisco Catalyst SD-WAN Manager Release 20.15.1 to 20.15.4 with Cisco IOS XE Catalyst SD-WAN devices running 17.14.x or earlier, use the **permit-v1** and **permit-list** keywords for backward compatibility.

```
ip community-list standard TEST permit-v1 permit-list 10
```

If you are using Cisco Catalyst SD-WAN Manager Release 20.15.5 and later with Cisco IOS XE Catalyst SD-WAN devices running 17.14.x or earlier, use the **deprecated** keyword for backward compatibility:

```
ip community-list-deprecated standard TEST permit 10
```

Examples

This example creates a standard BGP community list named COMMS that permits BGP routes with the community values 10:10 and 20:20. When a route-map uses this list in a **match** statement, the permit entry requires a BGP route to carry both community values **10:10** and **20:20** to satisfy the match condition. The route can also possess other community attributes; their presence does not prevent a match as long as **10:10** and **20:20** are both present. If a route contains only one of these two communities, it will not match this specific permit entry.

```
ip community-list standard COMMS permit 10:10 20:20
route-map TEST_COMM permit 10
 match community COMMS
```

When a route-map uses this list in an **exact-match** statement, the permit requires BGP route to carry exactly **10:10** and **20:20** community values to satisfy the **exact-match** condition. If a route contains more than these two communities, the match will be rejected.

```
ip community-list standard COMMS permit 10:10 20:20
route-map TEST_COMM permit 10
 match community COMMS exact-match
```

ip dhcp client vendor-class

By default the DHCP client carries PID (Product ID) of the device in option-124. This default behaviour can be overridden by configuring below CLI:

ip dhcp client vendor-class [**mac-address** | **ascii** | **hex** | **disable**]

Syntax Description

mac-address	The mac address of the device.
ascii	The user defined string in ascii format.
hex	The user defined string in hexadecimal format.
disable	Disables sending option-124 to DHCP messages.

Command Default

By default option-124 carries PID of the device.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	This command was introduced.

Usage Guidelines

By default the DHCP client carries PID of the device in option-124. This default behaviour can be overridden by configuring the **ip dhcp client vendor-class** command.

Examples

The following example shows the configuration to override the decive PID with MAC address:

```
interface GigabitEthernet 0/0/0
    ip address dhcp
    ip dhcp client vendor-class mac-address
    !
```

The DHCP vendor-class option, overrides the Device PID with MAC Address.

The following example shows the configuration to override the device PID with user defined string in hex or in ascii format:

```
interface GigabitEthernet 0/0/0
    ip address dhcp
    ip dhcp client vendor-class hex aabbcc
    !
```

```
interface GigabitEthernet 0/0/0
    ip address dhcp
    ip dhcp client vendor-class ascii cisco
    !
```

The following example shows the configuration to disable option-124 in DHCP messages:

```
interface GigabitEthernet 0/0/0
    ip address dhcp
    ip dhcp client vendor-class disable
    !
```

ip dhcp conflict logging

To enable conflict logging on a Dynamic Host Configuration Protocol (DHCP) server, use the **ip dhcp conflict logging** command in global configuration mode. To disable conflict logging, use the **no** form of this command.

ip dhcp conflict logging

no ip dhcp conflict logging

This command has no arguments or keywords.

Command Default

Conflict logging is enabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	This command was introduced.

Usage Guidelines

A DHCP server database agent should be used to store automatic bindings. If a DHCP server database agent is not used, specify the **no ip dhcp conflict logging** command to disable the recording of address conflicts. By default, the DHCP server records DHCP address conflicts in a log file.

Example

The following example disables the recording of DHCP address conflicts:

```
Device(config)# no ip dhcp conflict logging
```

ip dhcp use

To control what information the Dynamic Host Configuration Protocol (DHCP) server accepts or rejects during address allocation, use the **ip dhcp use** command in global configuration mode.

To disable the use of Dynamic Host Configuration Protocol (DHCP) parameters during address allocation, use the no form of this command.

ip dhcp use { **class** | **vrf remote** }
no ip dhcp use class

Syntax Description

class	Specifies that the DHCP server use DHCP classes during address allocation.
vrf	Specifies whether the DHCP server ignores or uses the receiving VPN routing and forwarding (VRF) interface during address allocation.

Command Default

The DHCP server allocates addresses by default.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Qualified for use in Cisco vManage CLI templates.

Usage Guidelines

When the Cisco IOS DHCP server code is allocating addresses, you can use the **ip dhcp use** command to either enable or disable the use of VRF configured on the interface, or to configure DHCP classes. If you use the **no ip dhcp use class** command, the DHCP class configuration is not deleted.

For usage guidelines, see Cisco IOS XE `ip dhcp use` command.

Examples

The following example shows how to configure the DHCP server to use the relay agent information option during address allocation:

```
Device(config)# ip dhcp use class
```

The following example shows how to configure the DHCP server to enable the use of the VRF configured on the interface during address allocation:

```
Device(config)# ip dhcp use vrf remote
```

The following example shows how to configure the DHCP server to disable the use of class during address allocation:

```
Device(config)# no ip dhcp use class
```

ip dhcp smart-relay

To allow the Cisco Dynamic Host Configuration Protocol (DHCP) relay agent to switch the gateway address (giaddr field of a DHCP packet) to secondary addresses when there is no DHCPOFFER message from a DHCP server, use the **ip dhcp smart-relay** command in global configuration mode. To disable this smart-relay functionality and restore the default behavior, use the **no** form of this command.

ip dhcp smart-relay

no ip dhcp smart-relay

Syntax Description

This command has no arguments or keywords.

Command Default

Command is disabled

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.13.1a	This command was introduced.

Usage Guidelines

The DHCP relay agent attempts to forward the primary address as the gateway address. After three attempts and no response, the relay agent automatically switches to secondary addresses.

Example

The following example enables the DHCP relay agent to automatically switch to secondary address pools:

```
Device(config)# service dhcp
Device(config)# interface GigabitEthernet0/0
Device(config)# ip address 172.16.0.1 255.255.0.0
Device(config)# secondary ip address 192.168.255.254 255.255.0.0
Device(config)# ip helper-address 10.0.0.1
Device(config)# ip dhcp smart-relay
Device(config)# end
!
```

ip dhcp use hardware-address client-id

To set the hardware-address as a client-id on all dhcp requests, use the **ip dhcp use hardware-address client-id** command in global configuration mode. To remove the hardware-address as the client-id, use the **no** form of this command.

ip dhcp use hardware-address client-id
no ip dhcp use hardware-address client-id

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command is qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Subscriber-id, vrf-id, hardware-address can be used as client-id in DHCP requests. Use this **ip dhcp use hardware-address client-id** command to set the hardware-address as a client-id on all DHCP requests.

Examples

The following example shows how to set the client-id of dhcp requests to use the hardware-address.

```
Device(config)# ip dhcp use hardware-address client-id
```

Table 24: Related Commands

Commands	Description
ip dhcp use class	DHCP server to use the relay agent information option during address allocation.
ip dhcp use subscriber-id	DHCP server to use the subscriber-id information option during address allocation.
ip dhcp use vrf	DHCP server to use the VRF information option during address allocation.

ip directed-broadcast

To enable the translation of a directed broadcast to physical broadcasts, use the **ip directed-broadcast** interface configuration command. To disable this function, use the **no** form of this command.

ip directed-broadcast

no ip directed-broadcast

Syntax Description This command has no arguments or keywords.

Command Default Disabled; all IP directed broadcasts are dropped.

Command Modes Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release Amsterdam 17.2.1v	Qualified for use in Cisco vManage CLI templates

Usage Guidelines For the usage guidelines, see ip directed-broadcast.

Examples

```
csr8k(config)# interface GigabitEthernet 1.101
csr8k(config-if)# ip address 192.168.66.1
csr8k(config-if)# ip directed-broadcast
```

ip dns server

To enable the Domain Name System (DNS) server on a router, use the **ip dns server** command in global configuration mode. To disable the DNS server, use the **no** form of the command.

ip dns server
no ip dns server

Syntax Description This command has no arguments or keywords.

Command Default The DNS server is disabled.

Command Modes Global configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	Qualified for use in Cisco vManage CLI templates.

Usage Guidelines Use this command to enable the DNS server as needed.

Examples In the following example, the DNS server is enabled:

```
Device(config)# ip dns server
```

ip domain lookup

To enable the Domain Name Server (DNS) lookup feature, use the **ip domain-lookup** command. Use the **no** form of this command to disable this feature.

ip domain lookup
no ip domain lookup

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `ip domain lookup` command.

Examples

This example shows how to disable the DNS server lookup feature:

```
Device(config)# no ip domain-lookup
```

ip finger

To configure a system to accept Finger protocol requests (defined in RFC 742), use the **ip finger** command in global configuration mode. To disable this service, use the **no**form of this command.

ip finger
no ip finger

Command Default

Disabled

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Examples

The following example disables the Finger protocol:

```
Device(config)# no ip finger
```

ip helper-address

To enable forwarding of User Datagram Protocol (UDP) broadcasts, including Bootstrap Protocol (BOOTP), received on an interface, use the **ip helper-address** command in interface configuration mode. To disable forwarding of broadcast packets to specific addresses, use the**no** form of this command.

ip helper-address *address*
no ip helper-address *address*

Syntax Description

address	Destination broadcast or host address to be used when forwarding UDP broadcasts. There can be more than one helper address per interface.

Command Default

UDP broadcasts are not forwarded.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For the usage guidelines, see ip helper-address and dhcp-helper

DHCP helper addresses are not supported in VPN 0 / VPN 512.

Examples

The following example shows how to define an address that acts as a helper address:

```
Device(config)# interface GigabitEthernet 1.101
Device(config-if)# ip nbar protocol-discovery
Device(config-if)# ip helper-address 10.8.4.5
```

ip host

To define static hostname-to-address mappings in the Domain Name System (DNS) hostname cache for a DNS view, use the **ip host** command in global configuration mode. If the hostname cache does not exist yet, it is automatically created. To remove a hostname-to-address mapping, use the **no** form of this command.

ip host [**vrf** *vrf-name*] [*ip-address1* . . . [*ip-addressn*]]
no ip host [**vrf** *vrf-name*] [*ip-address1* . . . [*ip-addressn*]]

Syntax Description

vrf *vrf-name*	(Optional) The *vrf-name* argument specifies the name of the Virtual Private Network (VRF) routing and forwarding (VRF) instance whose hostname cache is to store the mappings. Default is the global VRF (that is, the VRF whose name is a NULL string).

hostname	Name of the host. The first character can be either a letter or a number. If you use a number, the types of operations you can perform (such as ping) are limited.
ip-address1 . . . *ip-addressn*	Associated host IP address. You can specify an IPv4 or IPv6 address for the host IP address and additional IP addresses. (Optional) Additional associated IP addresses, delimited by a single space. **Note** The ellipses in the syntax description are used to indicate a range of values. Do not use ellipses when entering host IP addresses.

Command Default

No static hostname-to-address mapping is added to the DNS hostname cache.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	Qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `ip host` command.

For backward compatibility of Cisco Catalyst SD-WAN Manager Release 20.15.1 and later with devices running Cisco IOS XE Catalyst SD-WAN Release 17.14.1a and earlier, when using CLI device templates or CLI add-on feature templates, use a different form of the **ip host** command. When pushing the CLI device templates or CLI add-on feature templates to the device in global configuration mode, use the following form of the **ip host** command with **ip-list** :

ip host *hostname* **ip-list** *ip-address*

The following example shows how to add a mapping entry to the hostname vbond.ubi.in and IPv4 address 10.0.0.0 with list of IP addresses associated with a hostname.

```
Device(config)# ip host vbond.ubi.in ip-list 10.0.0.0
```

Examples

The following example shows how to add two mapping entries to the hostname that is associated with the VRF 101 and then remove one of those entries from that hostname cache:

```
Device(config)# ip host vrf 101 test-1 192.0.2.141 192.0.2.241
Device(config)# no ip host vrf 101 test-1 192.0.2.141
```

ip host *ip-address*

To define static hostname-to-address mappings in the Domain Name System (DNS) hostname cache for a DNS view, use the **ip host** command in global configuration mode. If the hostname cache does not exist yet, it is automatically created. To remove a hostname-to-address mapping, use the **no** form of this command.

ip host [*ip-address1* **. . .** [*ip-addressn*]]
no ip host [*ip-address1* **. . .** [*ip-addressn*]]

Syntax Description

ip-address1 **. . .***ip-addressn*	IP address of Cisco Catalyst SD-WAN Validator. You can specify an IPv4 or IPv6 address for the host IP address and additional IP addresses. (Optional) Additional associated IP addresses, delimited by a single space. You can configure a maximum of 24 IP addresses. **Note** The ellipses in the syntax description are used to indicate a range of values. Do not use ellipses when entering host IP addresses.

Command Default

No static hostname-to-address mapping is added to the DNS hostname cache.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	Qualified for use in Cisco vManage CLI templates.

Examples

The following example shows how to add two Cisco Catalyst SD-WAN Validator IP addresses as IP hosts, and how to remove one of them.

```
Device(config)# ip host 192.0.2.141 192.0.2.241

Device(config)# no ip host 192.0.2.141
```

ip http authentication

To specify a particular authentication method for HTTP server users, use the **ip http authentication** command in global configuration mode. To disable a configured authentication method, use the **no** form of this command.

ip http authentication local
no ip http authentication [**local**]

Syntax Description

local	Indicates that the login user name, password and privilege level access combination specified in the local system configuration (by the **username** global configuration command) should be used for authentication and authorization.

Command Default

The “enable” password is required when users (clients) connect to the HTTP server. Three command privilege levels exist on the router.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `ip http authentication` command.

Examples

The following example shows how to specify that the login user name, password and privilege level access combination specified in the local system configuration should be used for authentication and authorization.

```
Device(config)# ip http authentication local
```

ip http client source-interface

To enable HTTP client on your IP or IPv6 system, use the **ip http client** command in global configuration mode. To disable the HTTP client, use the **no** form of this command.

Supported Parameters

type	Name of the source interface.
number	Number of the source interface.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE ip http client source-interface command.

Example

```
Device(config)# ip http client source-interface GigabitEthernet0/0/2
```

ip http secure-server

To enable a secure HTTP (HTTPS) server, use the **ip http secure-server** command in global configuration mode. To disable an HTTPS server, use the **no** form of this command.

ip http secure-server
no ip http secure-server

Syntax Description

This command has no arguments or keywords.

Command Default

The HTTPS server is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `ip http secure-server` command.

Examples

In the following example the HTTPS server is disabled:

```
Device(config)# no ip http secure-server
```

ip http server

To enable the HTTP server on your IP or IPv6 system, including the Cisco web browser user interface, use the **ip http server**command in global configuration mode. To disable the HTTP server, use the **no** form of this command.

ip http server
no ip http server

Syntax Description

This command has no arguments or keywords.

Command Default

The HTTP server is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE`ip http server` command.

Examples

The following example shows how to disable the HTTP server:

```
Device(config)#no ip http server
```

ip http tls-version

To configure TLS version for HTTPS Server and HTTPS client sessions, use the **ip http tls-version** command in global configuration mode. To remove the configuration, use the **no** form of this command.

ip http tls-version *tls-version*
no ip http tls-version *tls-version*

Syntax Description

tls-version	Specifies TLS versions—TLSv1.0, TLSv1.1, TLSv1.2, and TLSv1.3.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	This command was introduced.

Usage Guidelines

The **ip http tls-version** command allows you to set a particular version used for HTTP secure-server sessions. The underlying SSL infrastructure supports the option of specifying either all or only one TLS version. Hence the HTTPS provides the option to specify the individual version.

By default, three TLS versions used for HTTPS sessions are supported—TLSv1.2 and TLSv1.3. To enable a particular version use this command.

Examples

The following shows how to configure TLS version 1.0 for the HTTPS session:

```
Device(config)# ip http tls-version TLSv1.0
```

ip icmp rate-limit unreachable

To limit the rate at which Internet Control Message Protocol (ICMP) unreachable messages are generated for a destination, use the **ip icmp rate-limit unreachable** command in global configuration mode.

To use the default, use the **no** form of this command.

ip icmp rate-limit unreachable *ms*
no ip icmp rate-limit unreachable

Syntax Description

ms	The optional ms argument is a time limit in milliseconds (ms) in which one unreachable message is generated. The valid range is from 1 ms to 4294967295 ms. **Note** Counting begins as soon as this command is configured.

Command Default The default value is one ICMP destination unreachable message per 500 ms.

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines For usage guidelines, see the Cisco IOS XE ip icmp rate-limit unreachable command.

Examples

The following example sets the rate of the ICMP destination unreachable message to one message every 10 ms:

```
Device(config)# ip icmp rate-limit unreachable 10
```

The following example turns off the previously configured rate limit:

```
Device(config)# no ip icmp rate-limit unreachable
```

ip icmp redirect

To control the type of Internet Control Message Protocol (ICMP) redirect message that is sent, use the **ip icmp redirect** command in global configuration mode. To set the value back to the default, use the **no**form of this command.

ip icmp redirect { **host** | **subnet** }
no ip icmp redirect

Syntax Description

host	Sends ICMP host redirects.
subnet	Sends ICMP subnet redirects.

Command Default The router will send ICMP subnet redirect messages.

Because the **ip icmp redirect subnet** command is the default, the command will not be displayed in the configuration.

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.3.1aexit	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines For usage guidelines, see the Cisco IOS XE ip icmp redirect command.

Examples

The following example enables the router to send out ICMP host redirects:

```
Device(config)# ip icmp redirect host
```

The following example sets the value back to the default, which is subnet redirects:

```
Device(config)# ip icmp redirect subnet
```

ip igmp ssm-map query dns

To configure Domain Name System (DNS)-based Source Specific Multicast (SSM) mapping, use the **ip igmp ssm-map query dns** command in global configuration mode. To disable DNS-based SSM mapping, use the **no** form of this command.

ip igmp ssm-map query dns
no ip igmp ssm-map query dns

Syntax Description

This command has no arguments.

Command Default

This command is enabled by default when the **ip igmp ssm-map enable** command is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE ip igmp ssm-map query dns command.

Examples

The following example shows how to disable DNS-based SSM mapping:

```
Device(config)# no ip igmp ssm-map query dns
```

ip load-sharing algorithm

To enable load balancing algorithm on an interface for IPv4, use the **ip load-sharing algorithm** command in Cisco Catalyst SD-WAN configuration mode. To disable load balancing algorithm on an interface, use the **no** form of this command.

ip load-sharing algorithm { ip-and-ports | src-dst-ip | src-ip-only }
no ip load-sharing algorithm { ip-and-ports | src-dst-ip | src-ip-only }

Syntax Description

ip-and-ports	Sets the load-balancing algorithm to the include-ports algorithm that uses Layer 4 source and destination ports.

src-dst-ip	Sets the load-balancing algorithm to the src-dst-ip algorithm that uses a source and destination ip.
src-ip-only	Sets the load-balancing algorithm to the src-ip algorithm that uses source ip.

Command Default

src-dst-ip algorithm is enabled by default.

Command Modes

SD-WAN configuration (config-sdwan)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	This command was introduced.

Usage Guidelines

When the load-balancing algorithm is set to src-dst-ip mode, each router on the network can make a different load sharing decision for each source-destination address pair.

The ip-and-ports algorithm allows you to use the Layer 4 source and destination ports as part of the load-balancing decision. This method benefits traffic streams running over equal-cost paths that are not loadshared because the majority of the traffic is between peer addresses that use different port numbers, such as Real-Time Protocol (RTP) streams.

Examples

The following example shows how to enable load-balancing algorithm for source, destination ip and port:

```
Device(config)# sdwan
Device(config-sdwan)# ip load-sharing algorithm ip-and-ports
```

The following example shows how to enable load balancing algorithm for source, destination ip:

```
Device(config)# sdwan
Device(config-sdwan)# ip load-sharing algorithm src-dst-ip
```

The following example shows how to enable load balancing algorithm for source ip only:

```
Device(config)# sdwan
Device(config-sdwan)# ip load-sharing algorithm src-ip-only
```

ip mtu

To set the maximum transmission unit (MTU) size of IP packets that are sent on an interface, use the **ip mtu** command in interface configuration mode. To restore the default MTU size, use the **no** form of this command.

ip mtu *bytes*
no ip mtu

Syntax Description

bytes	MTU size, in bytes.

Command Default

The default MTU value depends on the interface type.

Table 25: Default MTU Values by Interface Type

Interface Type	Default MTU (Bytes)
ATM	4470
Ethernet	1500
FDDI	4470
High-Speed Serial Interface High Speed Access (HSSI HSA)	4470
Serial	1500
Token Ring	4464
VRF-Aware Service Infrastructure (VASI)	9216

Command Modes

Interface configuration (config-if)
Subinterface configuration (config-subif)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For the usage guidelines, see the IOS XE ip mtu command.

Examples

```
Device(config)# interface GigabitEthernet 1
Device(config-if)# ip mtu 1500
```

```
Device(config)# interface ATM 0/2/0.1 point-to-point
Device(config-if)# ip mtu 1500
```

ip multicast route-limit

To limit the number of multicast routes (mroutes) that can be added to a multicast routing table, use the **ip multicast route-limit**command in global configuration mode. To disable this configuration, use the **no** form of this command.

ip multicast route-limit *limit*
no ip multicast route-limit *limit*

Syntax Description

limit	The number of mroutes that can be added. The range is from 1 to 2147483647. The default is 2147483647.

Command Default

limit : 2147483647

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

The **ip multicast route-limit** command limits the number of multicast routes that can be added to a router and generates an error message when the limit is exceeded.

For usage guidelines, see the Cisco IOS XE `ip multicast route-limit` command.

Examples

The following example shows how to set the mroute limit to 200,000:

```
Device(config-transaction)# ip multicast route-limit 200000
```

ip name-server

To specify the address of one or more name servers to use for name and address resolution, use the **ip name-server** command in global configuration mode. To remove the addresses specified, use the **no** form of this command.

ip name-server [**vrf** *server-address*]
no ip name-server [**vrf** *server-address*]

Syntax Description

vrf	Defines a virtual private network's routing and forwarding instance (VRF) table.
server-address	IPv4 address of a name server.
server-ip-list	List of IPv4 addresses separated by a comma.

Command Default

No name server addresses are specified.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `ip name-server` command.

For backward compatibility of Cisco Catalyst SD-WAN Manager Release 20.12.1 with devices running Cisco IOS XE Catalyst SD-WAN Release 17.11.1a, when using CLI device templates or CLI add on feature templates, use a different form of **ip name-server** command. If **ip name-server** command is configured in VRF, use the following form of the command:

ip name-server vrf *vrf* **server-ip-list** *list of DNS servers*

If **ip name-server** command is configured in a global mode, use **ip name-server no-vrf** *list of DNS servers*

Examples

The following example shows how to specify IPv4 host 10.0.0.0 as the name server:

```
Device(config)# ip name-server 10.0.0.0
```

ip pim

To enable Protocol Independent Multicast (PIM) on an interface, use the **ip pim** command in interface configuration or virtual network interface configuration mode. To disable PIM on the interface, use the **no** form of this command.

Supported Parameters

sparse-mode	Enables sparse mode of operation.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE ip pim command.

Examples

```
ip pim vrf 1 bsr-candidate GigabitEthernet5
ip pim vrf 1 rp-address 172.16.255.116
ip pim vrf 1 rp-candidate GigabitEthernet5 interval 10 priority 5

ip pim sparse-mode

spt-only
```

ip pim bsr-candidate

To configure a router to announce its candidacy as a bootstrap router (BSR), use the **ip pim bsr-candidate** command in global configuration mode. To remove this router as a BSR candidate, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **bsr-candidate** *interface-type interface-number* [*hash-mask-length* [*priority* [**accept-rp-candidate** [*acl-number acl-name*]]]]

no ip pim [**vrf** *vrf-name*] **bsr-candidate** *interface-type interface-number* [*hash-mask-length* [*priority* [**accept-rp-candidate** [*acl-number acl-name*]]]]

Syntax Description

vrf *vrf-name*	(Optional) Configures the router to announce its candidacy as a BSR for the multicast virtual private network's (MVPN) multicast routing and forwarding instance (MVRF) specified for the *vrf-name* argument.

interface-type interface-number	Interface type and number of the router from which the BSR address is derived. This address is sent in BSR messages. **Note** This interface must be enabled for Protocol-Independent Multicast (PIM) using the **ip pim** command.
hash-mask-length	(Optional) Length of a mask (32 bits maximum) that is to be combined with the group address before the PIMv2 hash function is called. All the groups with the same seed hash correspond to the same rendezvous point (RP). For example, if this value is 24, only the first 24 bits of the group addresses matter. The hash mask length allows one RP to be used for multiple groups. The default hash mask length is 0.
priority	(Optional) Priority of the candidate BSR (C-BSR). The range is from 0 to 255. The default priority is 0. The C-BSR with the highest priority value is preferred. **Note** The Cisco IOS and Cisco IOS XE implementation of PIM BSR uses the value 0 as the default priority for candidate BSRs. This implementation predates RFC 5059, which specifies that 64 be used as the default priority value. The Cisco IOS and Cisco IOS XE implementation, thus, deviates from RFC 5059. To comply with the default priority value specified in the RFC, you must explicitly set the priority value to 64.
accept-rp-candidate	(Optional) Specifies that the C-RP candidate is to be filtered.
acl-number	(Optional) Number of the access control list (ACL) to be used to filter C-RP advertisements. The range is 100 to 199 for standard ACL numbers and 2000 to 2699 for extended ACLs. **Note** You must have a valid standard or extended ACL in order to use an ACL in your configuration.
acl-name	(Optional) Name of the ACL to be used to filter C-RP advertisements. **Note** You must have a valid standard or extended ACL in order to use an ACL in your configuration.

Command Default

The router is not configured to announce itself as a candidate BSR.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE ip pim bsr-candidate command.

Examples

The following example shows how to configure the IP address of a router on GigabitEthernet interface 0/0 to be a BSR C-RP with a hash mask length of 0 and a priority of 192:

```
Device(config)# ip pim vrf 1 bsr-candidate GigabitEthernet 0/0 0 192
```

ip pim rp-address

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

Supported Parameters

vrf *vrf-name*	(Optional) Specifies that the static group-to-RP mapping be associated with the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
rp-address	IP address of the RP to be used for the static group-to-RP mapping. This is a unicast IP address in four-part dotted-decimal notation.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE ip pim rp-address command.

Examples

```
ip pim vrf 1 bsr-candidate GigabitEthernet5
ip pim vrf 1 rp-address 172.16.255.116
ip pim vrf 1 rp-candidate GigabitEthernet5 interval 10 priority 5

ip pim sparse-mode

spt-only
```

ip pim rp-candidate

To configure a router to advertise itself to the bootstrap router (BSR) as a Protocol-Indepedenet Multicast (PIM) Version 2 (PIMv2) candidate rendezvous point (C-RP), use the **ip pim rp-candidate** command in global configuration mode. To remove this router as a C-RP, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **rp-candidate** *interface-type interface-number* [**group-list** *access-list*] [**interval** *seconds*] [**priority** *value*]

no ip pim [**vrf** *vrf-name*] **rp-candidate**

Syntax Description

vrf *vrf-name*	(Optional) Configure the router to advertise itself to the BSR as PIMv2 C-RP for the multicast virtual private network's (MVPN) multicast routing and forwarding instance (MVRF) specified for the *vrf-name* argument.
interface-type interface-number	IP address associated with this interface type and number to be advertised as a C-RP address.
group-list *access-list*	(Optional) Specifies the standard IP access list number or name that defines the group prefixes that are advertised in association with the RP address. The access list name cannot contain a space or quotation mark, and must begin with an alphabetic character to avoid confusion with numbered access lists. **Note** You must have a valid standard or extended ACL in order to use an ACL in your configuration.
interval *seconds*	(Optional) Specifies the C-RP advertisement interval, in seconds. The range is from 1 to 16383. The default value is 60.
priority *value*	(Optional) Specifies the priority of the C-RP. The range is from 0 to 255. The default priority value is 0. The BSR C-RP with the lowest priority value is preferred. **Note** The Cisco IOS and Cisco IOS XE implementation of PIM BSR uses the value 0 as the default priority for candidate RPs. This implementation predates the draft-ietf-pim-sm-bsr IETF draft, the first IETF draft to specify 192 as the default priority value. The Cisco IOS and Cisco IOS XE implementation, thus, deviates from the IETF draft. To comply with the default priority value specified in the draft, you must explicitly set the priority value to 192.

Command Default

The router is not configured to announce itself to the BSR as a PIMv2 C-RP.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE ip pim rp-candidate command.

Examples

The following example shows how to configure a router 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 0/0. That RP is responsible for the groups with the prefix 239.

```
Device(config)# ip pim vrf 1 rp-candidate GigabitEthernet5 interval 10 priority 5
Device(config)# access-list 4 permit 239.0.0.0 0.255.255.255
```

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* **permit** *network / length*
no ip prefix-list *list-name* **permit** *network / length*

Syntax Description

list-name	Name to identify the prefix list. Do not use the words *detail* or *summary* as a list name because they are keywords in the **show ip prefix-list** command.
permit	Permits access for a matching condition.

Command Default

No prefix lists or prefix list entries are created.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `ip prefix-list` command.

Examples

In the following example, a prefix list is configured to permit the default route 10.0.0.0/8:

```
Device(config)# ip prefix-list TEST permit 10.0.0.0/8
```

ip redirects

To enable the task of sending Internet Control Message Protocol (ICMP) redirect messages if the software is forced to resend a packet through the same interface on which it was received, use the **ip redirects** command in interface configuration mode. To disable the task of sending redirect messages, use the **no** form of this command.

ip redirects
no ip redirects

Syntax Description

This command has no arguments or keywords.

Command Default

ICMP redirect messages are sent.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For the usage guidelines, see ip redirects.

Examples

The following example shows how to enable the sending of ICMP redirect messages on GigabitEthernet interface 1:

```
Device(config)# interface GigabitEthernet 1
Device(config-if)# ip redirects
```

The following example shows how to disable the sending of ICMP redirect messages on Tunnel interface 1:

```
Device(config)# interface Tunnel 1
Device(config-if)# no ip redirects
```

ip rcmd

To enable the IP remote command (rcmd) option, use the **ip rcmd** command in global configuration mode. To disable the IP remote command (rcmd) option, use the **no** form of this command.

ip rcmd { **domain-lookup** | **rcp-enable** | **rsh-enable** }
no ip rcmd { **domain-lookup** | **rcp-enable** | **rsh-enable** }

Syntax Description

domain-lookup Re-enables basic Domain Name System (DNS) security check for Remote Copy Protocol (RCP) and remote shell (rsh).

We recommend not including the ip **rcmd domain-lookup** command in a CLI add-on profile.

However, if you decide to use the **ip rcmd domain-lookup** command in a CLI add-on profile, do one of these to prevent an error:

- In the configuration group that you are using to push a configuration to the device, enable IP domain lookup.

  To do this: In the configuration group, open **System profile** > **Global** feature. Enable Domain Lookup.

- Alternatively, include the **ip domain lookup** command in the CLI add-on profile. This prevents the **ip rcmd domain-lookup** command from triggering an error.

  A simplified excerpt of a CLI add-on profile showing the two commands:

  ```
  ip domain lookup
  ip rcmd domain-lookup
  ```

  Note
  Executing the **show running-config** command on a device does not show the **ip domain lookup** command in the output even if it is configured. However, with the **all** keyword, the **show running-config all** command output does show the **ip domain lookup** command if configured.

rcp-enable	Allows remote users to copy files to and from the router using RCP.
rsh-enable	Allows remote users to execute commands on it using rsh.

Command Default

Domain-lookup is enabled.

rcp-enable is disabled.

rsh-enable is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

The abbreviation RCMD (remote command) is used to indicate both rsh and RCP. DNS lookup for RCMD is enabled by default and is performed as a basic security check. RCP-enable allows a remote user to execute RCP commands on the router. rsh, used as a client process, gives users the ability to remotely get router information, such as status, without the need to connect to the router and then disconnect. RSH-enable enables the router to receive rsh requests from remote users.

Examples

The following example shows how to enable RCP and rsh.

```
Device(config)# ip rcmd rcp-enable
Device(config)# ip rcmd rsh-enable
```

ip rcmd rcp-enable

To allow remote users to copy files to and from a router using Remote Copy Protocol (RCP), use the **ip rcmd rcp-enable** command in global configuration mode. To disable RCP on the device, use the **no** form of this command.

ip rcmd rcp-enable
no ip rcmd rcp-enable

Syntax Description

This command has no arguments or keywords.

Command Default

To ensure security, the router is not enabled for RCP by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `ip rcmd rcp-enable` command.

Examples

The following example shows how to enable RCP for copying files to and from a router:

```
Device(config)#ip rcmd rcp-enable
```

ip rcmd rsh-enable

To configure a router to allow remote users to execute commands on it using remote shell protocol (rsh), use the **ip rcmd rsh-enable** command in global configuration mode. To disable a router that is enabled for rsh, use the **no** form of this command.

ip rcmd rsh-enable
no ip rcmd rsh-enable

Syntax Description

This command has no arguments or keywords.

Command Default

To ensure security, the router is not enabled for rsh by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `ip rcmd rsh-enable` command.

Examples

The following example shows how to enable a router as an rsh server:

```
Device(config)# ip rcmd rsh-enable
```

ip route vrf

To establish static routes for a virtual private network's routing and forwarding (VRF) instance, use the **ip route vrf** command in global configuration mode. To disable static routes, use the **no** form of this command.

ip route vrf *vrf-name prefix mask* [*interface interface-number*] [*next-hop-address* [**tag** *tag*] [**track** *number*]]
no ip route vrf *vrf-name prefix mask* [*interface interface-number*] [*next-hop-address* [**tag** *tag*] [**track** *number*]]

Syntax Description

vrf-name	Name of the VRF for the static route.
prefix	IP route prefix for the destination, in dotted decimal format.
mask	Prefix mask for the destination, in dotted decimal format.

next-hop-address	(Optional) IP address of the next hop (the forwarding router that can be used to reach that network).
interface	(Optional) Name of network interface to use.
interface-number	(Optional) Number identifying the network interface to use.
tag *tag*	(Optional) Specifies the label (tag) value that can be used for controlling redistribution of routes through route maps.
track *number*	(Optional) Associates a track object with this route. Valid values for the number argument range from 1 to 500.

Command Default

No default behavior or values.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Additional parameters qualified: prefix mask for destination address, next-hop address, interface type and number, tag.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `ip route vrf` command.

Examples

```
Device (config)# ip route vrf 1 192.0.2.1 255.255.255.0 198.51.100.1 track 10
Device (config)# ip route vrf 1 192.0.2.1 255.255.255.0 198.51.100.1 tag 2
Device (config)# ip route vrf 1 192.0.2.1 255.255.255.0 198.51.100.1
Device (config)# ip route vrf 1 192.0.2.1 255.255.255.0 GigabitEthernet2
Device (config)# ip route vrf 1 192.0.2.1 255.255.255.0
```

ip route

To establish a static route, use the **ip route** command in global configuration mode. To remove static routes, use the **no** form of this command.

ip route *prefix mask* [*ip-address* | *interface-type-interface-number* [*ip-address*] | **Null0** *distance*] [**tag** *tag* | **track**]

no ip route *prefix mask* [*ip-address* | *interface-type-interface-number* [*ip-address*] | **Null0** *distance*] [**tag** *tag* | **track**]

Syntax Description

prefix	IP route prefix for the destination.
mask	Prefix mask for the destination.
ip-address	IP address of the next hop that can be used to reach the network.

interface-type interface-number	Network interface type and interface number. Valid values for the *number* argument range from 1 to 500.
track	(Optional) Associates a track object with this route.
tag *tag*	(Optional) Tag value that can be used as a match value for controlling redistribution through route maps.
Null0	Specifies null0 as the interface to prevent routing loops.
distance	(Optional) Administrative distance. The range is 1 to 255. The default administrative distance for a static route is 1.

Command Default

No static routes are established.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Additional parameters qualified: next-hop-address, Dialer, tag, track, Null0, distance.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `ip route`command.

Examples

The following example shows how to route packets for network 192.0.2.1 to a router at 198.51.100.1:

```
ip route 192.0.2.1 255.255.255.0 198.51.100.1
```

```
Device(config)# ip route 192.0.2.1 255.255.255.0 198.51.100.1 track <>
ip route 192.0.2.1 255.255.255.0 Dialer2 198.51.100.1 tag <>
ip route 192.0.2.1 255.255.255.0 198.51.100.1 tag <>
ip route 192.0.2.1 255.255.255.0 Dialer2 tag <>
ip route 192.0.2.1 255.255.255.0 Dialer2 198.51.100.1 <>
ip route 192.0.2.1 255.255.255.0 198.51.100.1 <>
ip route 192.0.2.1 255.255.255.0 Dialer2 <>
ip route 192.0.2.1 255.255.255.0 GigabitEthernet2 <>
ip route 192.0.2.1 255.255.255.0 <>
```

ip source-route

To allow the Cisco IOS software to handle IP datagrams with source-routing header options, use the **ip source-route** command in global configuration mode. To have the software discard any IP datagram containing a source-route option, use the **no** form of this command.

ip source-route
no ip source-route

Syntax Description

This command has no arguments or keywords.

Command Default Enabled

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Examples

The following example shows how to disable the handling of IP datagrams with source-routing header options:

```
Device(config)# no ip source-route
```

ip ssh version

To specify the version of Secure Shell (SSH) to be run on a router, use the **ip ssh version**command in global configuration mode. To disable the version of SSH that is configured and to return to compatibility mode, use the **no** form of this command.

ip ssh version 2
no ip ssh version

Syntax Description

2	Router runs only SSH Version 2.

Command Default If this command is not configured, SSH operates in compatibility mode, that is, Version 1 and Version 2 are both supported.

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines Use this command with the keyword **2** to ensure that your router will not inadvertently establish a weaker SSH Version 1 connection.

Examples

The following example shows that SSH Version 2 support is configured:

```
Router (config-transaction)# ip ssh version 2
```

The following example shows that SSH Version 2 configuration is removed:

```
Router (config-transaction)# no ip ssh version
```

ip tcp adjust-mss

To adjust the maximum segment size (MSS) value of TCP synchronize/start (SYN) packets that go through a router, use the **ip tcp adjust-mss** command in interface configuration mode. To return the MSS value to the default setting, use the **no** form of this command.

ip tcp adjust-mss *max-segment-size*
no ip tcp adjust-mss

Syntax Description

max-segment-size	Maximum segment size, in bytes. The range is from 500 to 1460.

Command Default

The MSS is determined by the originating host.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For the usage guidelines, see ip tcp adjust-mss.

Examples

```
Device(config)# interface GigabitEthernet 1
Device(config-if)# ip tcp adjust-mss 1100
```

ip tcp mss

To enable a maximum segment size (MSS) for TCP connections originating or terminating on a router, use the **ip tcp mss** command in global configuration mode. To disable the configuration of the MSS, use the no form of this command.

ip tcp mss *bytes*
no ip tcp mss

Syntax Description

bytes	Maximum segment size for TCP connections in bytes. Valid values are from 0 to 10000.

Command Default

This command is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `ip tcp mass` command.

Examples

The following example sets the MSS value at 1200:

```
Device(config)# ip tcp mss 1200
```

ip unnumbered

To enable IP processing on an interface without assigning an explicit IP address to the interface, use the **ip unnumbered** command in interface configuration mode or subinterface configuration mode. To disable the IP processing on the interface, use the **no** form of this command.

ip unnumbered *type*
no ip unnumbered

Syntax Description

type	Type of interface. For more information, use the question mark (**?**) online help function.

Command Default

Unnumbered interfaces are not supported.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE ip unnumbered command.

Examples

The following example shows how to configure GigabitEthernet 1 as an IP unnumbered interface.

```
Device(config)# interface Tunnel 1
Device(config-if)# ip unnumbered GigabitEthernet1
```

ip virtual-reassembly

ip virtual-reassemly command is used to enable a virtual packet reassembly on a Cisco IOS XE Catalyst SD-WAN device's interface. Virtual packet reassembly is a mechanism that helps in handling fragmented packets. To disable virtual reassembly, use the **no** form of this command.

ip virtual-reassembly [**max-reassemblies** *number*] [**max-fragments** *number*] [**timeout** *seconds*] [**drop-fragments**]

no ip virtual-reassembly [**max-reassemblies** *number*] [**max-fragments** *number*] [**timeout** *seconds*] [**drop-fragments**]

Syntax Description

max-reassemblies	(Optional) The number specifies the maximum number of IP packet reassemblies that can be held in the reassembly queue.
max-fragments	(Optional) The number specifies the upper limit on the number of fragments that can be created from a single IP packet.
timeout	(Optional) The timeout parameter defines the time window during which all fragments belonging to a particular IP packet are expected to arrive.
drop-fragments	(Optional) The drop-fragments parameter allows you to specify how the router should handle alone fragments that do not belong to any active reassembly process.

Command Default Disabled; all IP directed virtual fragmentation are dropped.

Command Modes Interface Configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	Qualified for use in Cisco vManage CLI templates

Example

This example shows how to enable virtual reassemly:

```
Device# config-transaction
Device(config)#interface GigabitEthernet 3
Device(config-if)#ip virtual-reassembly max-reassemblies 3
Device(config-if)#ip virtual-reassembly max-reassemblies 3 max-fragments 60
```

ipv6 access-class

To create or configure an IPv6 access class to restrict incoming or outgoing traffic on a virtual terminal line (VTY), use the **ipv6 access-class** command. To remove the access class, use the **no** form of this command

ipv6 access-class *access-list-name*

no ipv6 access-class

Syntax Description

Syntax Description

access-list-name	Name of the IPv6 ACL class. The name can be a maximum of 64 characters. The name can contain characters, numbers, hyphens, and underscores. The name cannot contain a space or quotation mark.

Command Default

None

Command Modes

Line configuration mode (config-line)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `ipv6 access-class` command.

Examples

This example shows how to configure an access class on a VTY line:

```
Device(config)# line vty 0 4
Device(config-line)# ipv6 access-class TEST
```

ipv6 address

To configure an IPv6 address and enable IPv6 processing on an interface, use the **ipv6 address** command in interface configuration mode. To remove the address from the interface, use the **no** form of this command.

ipv6 address *ipv6-address*
no ipv6 address *ipv6-address*

Syntax Description

ipv6-address	The IPv6 address to be used.

Command Default

No IPv6 addresses are defined for any interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For the usage guidelines, see the Cisco IOS ipv6 address command.

Examples

```
Device(config)# interface GigabitEthernet 1.101
Device(config-if)# ipv6 address 2001:DB8::1
```

ipv6 address autoconfig

To enable automatic configuration of IPv6 addresses using stateless autoconfiguration on an interface and enable IPv6 processing on the interface, use the **ipv6 address autoconfig** command in interface configuration mode. To remove the address from the interface, use the **no** form of this command.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE ipv6 address autoconfig command.

Examples

The following example assigns the IPv6 address automatically:

```
Device(config)# interface ethernet 0
Device(config-if)# ipv6 address autoconfig
```

ipv6 address dhcp client request

To configure an IPv6 client to request a vendor-specific option from a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server, use the **ipv6 address dhcp client request** command in interface configuration mode. To remove the request, use the **no** form of this command.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE ipv6 address dhcp client request command.

Examples

The following example shows how to configure an interface to request vendor-specific options:

```
Device(config)# interface fastethernet 0/0
Device(config-if)# ipv6 address dhcp client request vendor
```

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 { **universal** [*id*] | **include-ports** [**source** [*id*] | **destination** [*id*]] | **src-only** [*id*] }
no ipv6 cef load-sharing algorithm

universal*[id]*	Sets the load-balancing algorithm to the universal algorithm that uses a source and destination IP. (This is set as default).
id	(Optional) Fixed identifier.
include-ports {**source***[id]* | **destination***[id]*}	Sets the load-balancing algorithm to one that uses the source port and destination port.
src-only *[id]*	Sets the load-balancing algorithm to include source-only port.

Command Default

The universal load-balancing algorithm is selected. 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 Catalyst SD-WAN Release 17.6.1a	This command was introduced.
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	This command was modified. The **src-only** algorithm is added.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE ipv6 cef load-sharing algorithm command.

You can enable **ECMP keying** to send the configurations for both IPv4 and IPv6.

Examples

The following example shows how to enable the IPv6 CEF load-balancing algorithm for universal:

```
Device# config-transaction
Device (config-if)# ipv6 cef load-sharing algorithm universal
```

The following example shows how to enable the IPv6 CEF load-sharing algorithm for include-ports:

```
Device# config-transaction
Device(config)# ipv6 cef load-sharing algorithm include-ports source destination
```

The following example shows how to enable IPv6 CEF load-sharing algorithm to src-only port algorithm:

```
Device# config-transaction
Device(config)# ipv6 cef load-sharing algorithm src-only

Device(config)# commit
```

ipv6 dhcp client pd

To enable the Dynamic Host Configuration Protocol (DHCP) for IPv6 client process and enable request for prefix delegation through a specified interface, use the **ipv6 dhcp client pd** command in interface configuration mode. To disable requests for prefix delegation, use the **no** form of this command.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE ipv6 dhcp client pd command.

Examples

The following example enables prefix delegation:

```
Device(config-if)# ipv6 dhcp client pd dhcp-prefix
```

The following example configures a hint for prefix-delegating routers:

```
Device(config-if)# ipv6 dhcp client pd hint 2001:0DB8:1/48
```

ipv6 dhcp client vendor-class

By default the DHCP client carries PID (Product ID) of the device in option-16. This default behaviour can be overridden by configuring below CLI:

ipv6 dhcp client vendor-class [**mac-address** | **ascii** | **hex** | **disable**]

Syntax Description

mac-address	The mac address of the device.
ascii	The user defined string in ascii format.
hex	The user defined string in hexadecimal format.
disable	Disables sending option-16 to DHCP messages.

Command Default

By default option-16 carries PID of the device.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	This command was introduced.

Usage Guidelines

By default the DHCP client carries PID of the device in option-16. This default behaviour can be overridden by configuring the **ipv6 dhcp client vendor-class** command.

Examples

The following example shows the configuration to override the decive PID with MAC address:

```
interface GigabitEthernet 0/0/0
    ipv6 address dhcp
    ipv6 dhcp client vendor-class mac-address
    !
```

The DHCPv6 vendor-class option, overrides the Device PID with MAC Address.

The following example shows the configuration to override the device PID with user defined string in hex or in ascii format:

```
interface GigabitEthernet 0/0/0
    ipv6 address dhcp
    ipv6 dhcp client vendor-class hex aabbcc
    !
```

```
interface GigabitEthernet 0/0/0
    ipv6 address dhcp
    ipv6 dhcp client vendor-class ascii cisco
    !
```

The following example shows the configuration to disable option-16 in DHCP messages:

```
interface GigabitEthernet 0/0/0
    ipv6 address dhcp
    ipv6 dhcp client vendor-class disable
    !
```

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.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE ipv6 dhcp pool command.

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
```

The following example shows how to configure a pool named engineering with three link-address prefixes and an IPv6 address prefix:

```
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)#
Device(config-dhcpv6)# address prefix 2001:1003::0/64
```

The following example shows how to configure a pool named 350 with vendor-specific options:

```
Device(config)# ipv6 dhcp pool 350
Device(config-dhcpv6)# vendor-specific 9
Device(config-dhcpv6-vs)# suboption 1 address 1000:235D::1
Device(config-dhcpv6-vs)# suboption 2 ascii "IP-Phone"
```

ipv6 dhcp relay destination

To specify a destination address to which client messages are forwarded and to enable Dynamic Host Configuration Protocol (DHCP) for IPv6 relay service on the interface, use the **ipv6 dhcp relay destination** command in interface configuration mode. To remove a relay destination on the interface or to delete an output interface for a destination, use the **no** form of this command.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE ipv6 dhcp relay destination command.

Examples

The following example sets the relay destination address on Ethernet interface 4/3:

```
Device(config-if)# ipv6 dhcp relay destination FE80::250:A2FF:FEBF:A056 ethernet 4/3
```

The following example shows how to set the relay destination address on the Ethernet interface 4/3 on a Cisco CMTS router:

```
Device(config-if)# ipv6 dhcp relay destination 2001:db8:1234:5678:9abc:def1:2345:6789
ethernet 4/3
```

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.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE 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
```

ipv6 dhcp server

To enable Dynamic Host Configuration Protocol (DHCP) for IPv6 service on an interface, use the **ipv6 dhcp server** in interface configuration mode. To disable DHCP for IPv6 service on an interface, use the **no** form of this command.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE ipv6 dhcp server command.

Examples

The following example enables DHCP for IPv6 for the local prefix pool named server1:

```
Device(config-if)# ipv6 dhcp server server1
```

ipv6 enable

To enable IPv6 processing on an interface that has not been configured with an explicit IPv6 address, use the **ipv6 enable**command in interface configuration mode. To disable IPv6 processing on an interface that has not been configured with an explicit IPv6 address, use the **no** form of this command.

ipv6 enable
no ipv6 enable

Syntax Description

This command has no arguments or keywords.

Command Default

IPv6 is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release Amsterdam 17.2.1v	Qualified for use in Cisco vManage CLI templates.

Usage Guidelines

The **ipv6 enable**command automatically configures an IPv6 link-local unicast address on the interface while also enabling the interface for IPv6 processing. The no **ipv6 enable**command does not disable IPv6 processing on an interface that is configured with an explicit IPv6 address.

Examples

```
Device(config)# interface GigabitEthernet 1.101
Device(config-if)# ipv6 enable
```

ipv6 load-sharing algorithm

To enable load balancing algorithm on an interface for IPv6, use the **ipv6 load-sharing algorithm** command in Cisco Catalyst SD-WAN configuration mode. To disable load balancing algorithm on an interface, use the **no** form of this command.

ipv6 load-sharing algorithm { **ip-and-ports** | **src-dst-ip** | **src-ip-only** }
no ipv6 load-sharing algorithm { **ip-and-ports** | **src-dst-ip** | **src-ip-only** }

ip-and-ports	Sets the load-balancing algorithm to the include-ports algorithm that uses Layer 4 source and destination ports.
src-dst-ip	Sets the load-balancing algorithm to the src-dst-ip algorithm that uses a source and destination ip.
src-ip-only	Sets the load-balancing algorithm to the src-ip algorithm that uses source ip.

Command Default

src-dst-ip algorithm is enabled by default.

Command Modes

SD-WAN configuration (config-sdwan)

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	This command was introduced.

Usage Guidelines

When the load-balancing algorithm is set to src-dst-ip mode, each router on the network can make a different load sharing decision for each source-destination address pair.

The ip-and-ports algorithm allows you to use the Layer 4 source and destination ports as part of the load-balancing decision. This method benefits traffic streams running over equal-cost paths that are not loadshared because the majority of the traffic is between peer addresses that use different port numbers, such as Real-Time Protocol (RTP) streams.

Examples

The following example shows how to enable load-balancing algorithm for source, destination ip and port:

```
Device(config)# sdwan
Device(config-sdwan)# ipv6 load-sharing algorithm ip-and-ports
```

The following example shows how to enable load balancing algorithm for source, destination ip:

```
Device(config)# sdwan
Device(config-sdwan)# ipv6 load-sharing algorithm src-dst-ip
```

The following example shows how to enable load balancing algorithm for source ip only:

```
Device(config)# sdwan
Device(config-sdwan)# ipv6 load-sharing algorithm src-ip-only
```

ipv6 nd other-config-flag

To set the "other stateful configuration" flag in IPv6 router advertisements, use the **ipv6 nd other-config-flag** command in interface configuration mode. To clear the flag from IPv6 router advertisements, use the **no** form of this command.

ipv6 nd other-config-flag
no ipv6 nd other-config-flag

Command Default

None

Command Modes

interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

The setting of the "other stateful configuration" flag in IPv6 router advertisements indicates to attached hosts how they can obtain autoconfiguration information other than addresses. If the flag is set, the attached hosts should use stateful autoconfiguration to obtain the other (nonaddress) information.

Example

The following example configures the “other stateful configuration” flag in ipv6 router advertisements on GigabitEthernet 0/0/2.

```
Device(config)# interface GigabitEthernet 0/0/2
Device(config-if)# ipv6 nd other-config-flag
```

Table 26: Related Commands

Command	Description
ipv6 nd managed-config-flag	Sets the “managed address configuration” flag in ipv6 router advertisements.

ipv6 nd prefix

To configure ipv6 prefixes that are included in IPv6 neighbor discovery router advertisements, use the **ipv6 nd prefix** command in interface configuration mode. To remove the prefixes, use the **no** form of this command.

ipv6 nd prefix ipv6-prefix /prefix-length [**no-advertise**]
no ipv6 nd prefix ipv6-prefix /prefix-length [**no-advertise**]

Syntax Description

ipv6-prefix	Specifies the ipv6 network number to include the router advertisements (RA).
/ prefix-length	Specifies the length of the ipv6 prefix.

no-advertise	(Optional) specifies that the prefix is not advertised.

Command Default

All prefixes configured on interfaces that originate IPv6 router advertisements are advertised with a valid lifetime of 2,592,000 seconds (30 days) and a preferred lifetime of 604,800 seconds (7 days).

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

The **ipv6 nd prefix** command allows control over individual parameters per prefix, including whether the prefix should be advertised or not.

Example

The following example includes the ipv6 prefix 2001:0DB8::/35 in router advertisements sent out GigabitEthernet 0/0/2.

```
Device(config)# interface GigabitEthernet 0/0/2
Device(config-if)# ipv6 nd prefix 2001:0DB8::/35
```

ipv6 nd ra suppress

To suppress IPv6 router advertisement transmissions on an interface, use the **ipv6 nd ra suppress** command in interface configuration mode. To reenable the sending of IPv6 router advertisement transmissions on an interface, use the **no** form of this command.

ipv6 nd ra suppress [**all**]
no ipv6 nd ra suppress [**all**]

Syntax Description

all	(optional) suppress all router advertisements (RAs) on an interface.

Command Default

IPv6 router advertisements are automatically sent on Ethernet and FDDI interfaces if IPv6 unicast routing is enabled on the interfaces. IPv6 router advertisements are not sent on other types of interfaces.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

The **ipv6 nd ra suppress** command only suppresses periodic unsolicited RAs. It does not suppress RAs sent in response to a router solicitation. To suppress all RAs, including those sent in response to a router solicitation, use the **ipv6 nd ra suppress** command with the all keyword.

Example

The following example shows how to suppress IPv6 router advertisements on interface GigabitEthernet 0/0/2.

```
Device(config)# interface GigabitEthernet 0/0/2
Device(config-if)# ipv6 nd ra suppress
```

Table 27: Related Commands

Command	Description
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 nd router-preference

To configure a default router preference (DRP) for the router on a specific interface, use the **ipv6 nd router-preference** command in interface configuration mode. To return to the default DRP, use the **no** form of this command.

ipv6 nd router-preference { *high* | *medium* | *low* }
no ipv6 nd router-preference { *high* | *medium* | *low* }

Syntax Description

high	Preference for the router specified on an interface is high.
medium	Preference for the router specified on an interface is medium.
low	Preference for the router specified on an interface is low.

Command Default

Router Advertisements (RAs) are sent with the medium preference.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Router Advertisement messages are sent with the DRP configured by the **ipv6 nd router-preference** command. If no DRP is configured, Router Advertisements are sent with a medium preference. A DRP is useful when, for example, two routers on a link may provide equivalent, but not equal-cost, routing, and policy may dictate that hosts should prefer one of the routers.

Example

The following example configures a DRP of high for the router on GigabitEthernet 0/0/2.

```
Device(config)# interface GigabitEthernet 0/0/2
Device(config-if)# ipv6 nd router-preference High
```

ipv6 redirects

To enable the sending of Internet Control Message Protocol (ICMP) IPv6 redirect messages if Cisco IOS software is forced to resend a packet through the same interface on which the packet was received, use the **ipv6 redirects** command in interface configuration mode. To disable the sending of redirect messages, use the **no** form of this command.

ipv6 redirects
no ipv6 redirects

Syntax Description This command has no arguments or keywords.

Command Default The sending of ICMP IPv6 redirect messages is enabled.

Command Modes Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

Examples The following example disables the sending of ICMP IPv6 redirect messages on Tunnel interface 1:

```
Device(config)# interface Tunnel 1
Device(config-if)# ipv6 unnumbered GigabitEthernet0/2.101
Device(config-if)# no ipv6 redirects
```

Related Commands

Command	Description
ipv6 icmp error-interval	Configures the interval for IPv6 ICMP error messages.

ipv6 route

To establish static IPv6 routes, use the **ipv6 route**command in global configuration mode. To remove a previously configured static route, use the **no** form of this command.

ipv6 route vrf *vrf-name ipv6-prefix/prefix-length*
no ipv6 route vrf *vrf-name ipv6-prefix/prefix-length*

Syntax Description

ipv6-prefix	The IPv6 network that is the destination of the static route. Can also be a host name when static host routes are configured.

/ *prefix-length*	The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
vrf *vrf-name*	Specifies all virtual private network (VPN) routing/forwarding instance (VRF) tables or a specific VRF table for an IPv6 address.

Command Default

No static routes are established.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `ipv6 route` command.

Examples

The following example configures a static route for use in a VRF for IPv6:

```
ipv6 route vrf TEST 2001:DB8::/32
```

ipv6-strict-control

To configure IPv6 as a default option on Cisco IOS XE Catalyst SD-WAN devices, Cisco SD-WAN Manager, and Cisco Catalyst SD-WAN Controller, use the **ipv6-strict-control** command in system configuration mode. To remove the option from the interface, use the **no** form of this command.

ipv6-strict-control { *true* | *false* }
no ipv6-strict-control

Syntax Description

true	Enables IPv6 as the default connection option for connecting to Cisco SD-WAN Manager, Cisco Catalyst SD-WAN Controller, and Cisco IOS XE Catalyst SD-WAN devices.

Command Default

An IPv4 connection is defined for an interface.

Command Modes

System configuration (config-system)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	Qualified for use in Cisco SD-WAN Manager CLI templates.

Examples

The following example shows how to configure IPv6 as a default connection option on a Cisco IOS XE Catalyst SD-WAN device to connect to Cisco SD-WAN Manager and Cisco Catalyst SD-WAN Controller:

```
Device(config)# system
Device(config-system)# gps-location latitude 32.0
Device(config-system)# gps-location longitude -100.0
Device(config-system)# system-ip 10.16.255.14
Device(config-system)# domain-id 1
Device(config-system)# site-id 400
Device(config-system)# ipv6-strict-control true
Device(config-system)# admin-tech-on-failure
Device(config-system)# organization-name "Cisco"
Device(config-system)# vbond vbond
```

ipv6 unnumbered

To enable IPv6 processing on an interface without assigning an explicit IPv6 address to the interface, use the **ipv6 unnumbered**command in interface configuration mode. To disable IPv6 on an unnumbered interface, use the **no** form of this command.

ipv6 unnumbered *interface-type* **interface-number**
no ipv6 unnumbered

Syntax Description

interface-type	The interface type of the source address that the unnumbered interface uses in the IPv6 packets that it originates. The source address cannot be another unnumbered interface.
interface-number	The interface number of the source address that the unnumbered interface uses in the IPv6 packets that it originates.

Command Default

This command is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

IPv6 packets that are originated from an unnumbered interface use the global IPv6 address of the interface specified in the **ipv6 unnumbered** command as the source address for the packets. The **ipv6 unnumbered**

interface command is used as a hint when doing source address selection; that is, when trying to determine the source address of an outgoing packet.

Examples

```
Device(config)# interface Tunnel 1
Device(config-if)# ipv6 unnumbered GigabitEthernet0/2.101
```

lease

To configure the duration of the lease for an IP address that is assigned from a Cisco IOS Dynamic Host Configuration Protocol (DHCP) server to a DHCP client, use the **lease** command in DHCP pool configuration mode. To restore the default value, use the no form of this command.

lease *days* [*hours* [*minutes*]]
no lease

Syntax Description

days	Specifies the duration of the lease in numbers of days.
hours	(Optional) Specifies the number of hours in the lease. A *days* value must be supplied before you can configure an *hours* value.
minutes	(Optional) Specifies the number of minutes in the lease. A *days* value and an *hours* value must be supplied before you can configure a *minutes* value.
infinite	Specifies that the duration of the lease is unlimited.

Command Default

1 day

Command Modes

DHCP pool configuration (dhcp-config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Examples

The following example shows a 365 day lease:

```
Device (config)# ip dhcp pool POOL1
Device(dhcp-config)# lease 365 0 0
```

network (DHCP)

To configure the network number and mask for a Dynamic Host Configuration Protocol (DHCP) address pool primary subnet on a DHCP server, use the **network** command in DHCP pool configuration mode. To remove the subnet number and mask, use the **no** form of this command.

network *network-number* [*mask*]

Syntax Description

network-number	The IP address of the primary DHCP address pool.
mask	(Optional) The bit combination that renders which portion of the address of the DHCP address pool refers to the network or subnet and which part refers to the host.

Command Default

This command is disabled by default.

Command Modes

DHCP pool configuration (dhcp-config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `network (DHCP)` command.

Examples

The following example shows how to configure 255.255.255. 0 as the subnetwork number and mask of the DHCP pool named pool1.

```
Device(config)# ip dhcp pool pool1
Device(dhcp-config)# network 172.16.0.0 255.255.255.0
```

option (DHCP)

To configure DHCP server options, use the **option** command in DHCP pool configuration mode. To remove the options, use the **no** form of this command.

option *code* [**ip** *list-name*]
no option *code*

Syntax Description

code	Specifies the DHCP option code. The range is from 0 to 254.
ip *address*	Specifies an IP address. Up to eight IP addresses can be specified.
string	Hexadecimal value truncated to 180 characters entered. Each byte in hexadecimal character strings is two hexadecimal digits. Each byte can be separated by a period, colon, or white space.

Command Default

The default instance number is 0.

Command Modes

DHCP pool configuration (dhcp-config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Examples

The following example shows how to configure DHCP option 150 for an IP list containing two IP addresses.

```
Device(config)# ip dhcp pool POOL1
Device(dhcp-config)# option 150 ip 10.10.10.1 10.10.10.2
```

prefix-delegation

To specify a manually configured numeric prefix to be delegated to a specified client (and optionally a specified identity association for prefix delegation [IAPD] for that client), use the **prefix-delegation** command in DHCP for IPv6 pool configuration mode. To remove the prefix, use the **no** form of this command.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE prefix-delegation command.

Examples

The following example configures an IAPD for a specified client:

```
Device(config)# prefix-delegation 2001:0DB8::/64 00030001000BBFAA2408
```

prefix-delegation pool

To specify a named IPv6 local prefix pool from which prefixes are delegated to Dynamic Host Configuration Protocol (DHCP) for IPv6 clients, use the **prefix-delegation pool** command in DHCP for IPv6 pool configuration mode. To remove a named IPv6 local prefix pool, use the **no** form of this command.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE prefix-delegation pool command.

Examples

The following example specifies that prefix requests should be satisfied from the pool called client-prefix-pool. The prefixes should be delegated with the valid lifetime set to 1800 seconds, and the preferred lifetime is set to 600 seconds:

```
Device(config)# prefix-delegation pool client-prefix-pool lifetime 1800 600
```

spt-only

To configure multicast routing in Cisco SD-WAN to use shortest-path first trees (SPT) only, use the **spt-only** command in VRF configuration mode. To disable SPT-only use the **no** form of this command.

spt-only

no spt-only

This command has no keywords or arguments.

Command Default

SPT-only is not configured.

Command Modes

VRF configuration (config-vrf-<vrf-id>)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

Enable spt-only on all Cisco IOS XE SD-WAN devices that have Cisco SD-WAN multicast overlay configured for the VRF.

Example

```
Device(config)# sdwan multicast address-family ipv4 vrf 1
Device(config-vrf-1)# spt-only
```

vlan internal allocation policy

To configure the allocation direction of the internal VLAN, use the **vlaninternalallocationpolicy** command in global configuration mode. To return the default setting, use the **no** form of this command to return.

vlan internal allocation policy ascending
no vlan internal allocation policy

Syntax Description

ascending	Allocates internal VLANs from 1006 to 4094.

Command Default

ascending

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE vlan internal allocation policy command.

Examples

```
Device(config)# vlan internal allocation policy ascending
```

vendor-specific

To configures vendor-defined options for the IPv6 address pool, use the **vendor-specific** command in global configuration mode. To disable the feature, use the **no** form of this command.

vendor-specific *vendor-id*

Syntax Description

vendor-id	Specify an ID for the vendor.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Examples

The following example configures vendor-defined options for the IPv6 address pool:

```
Device(config)# vendor-specific 10
```

vrf (DHCP pool)

To associate the on-demand address pool with a VPN routing and forwarding instance (VRF) name, use the **vrf** command in DHCP pool configuration mode. To remove the VRF name, use the **no** form of this command.

vrf *name*
no vrf *name*

Syntax Description

name	Name of the VRF to which the address pool is associated.

Command Default

No default behavior or values

Command Modes

DHCP pool configuration (dhcp-config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

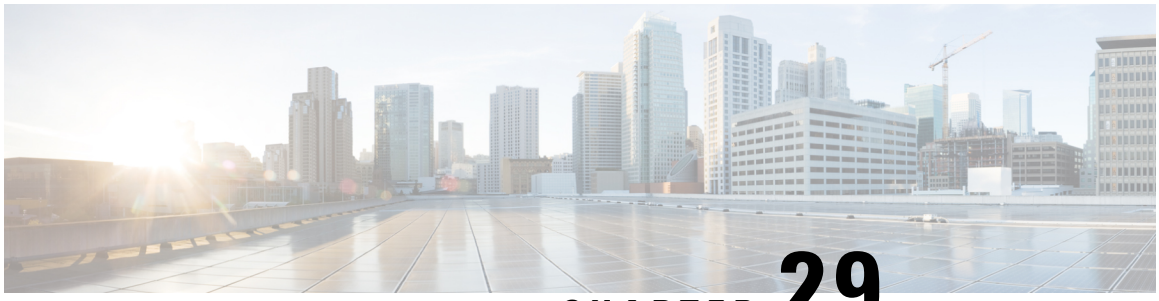
Usage Guidelines

For usage guidelines, see the Cisco IOS XE `vrf (DHCP Pool)` command.

Examples

The following example associates the address pool with a VRF named TEST:

```
Device(config)# ip dhcp pool POOL1
Device(dhcp-config)# vrf TEST
```



CHAPTER 29

IP Routing: OSPF Commands

- ip ospf area, on page 413
- ip ospf authentication, on page 414
- ip ospf cost, on page 414
- ip ospf dead-interval, on page 415
- ip ospf hello-interval, on page 415
- ip ospf message-digest-key md5, on page 416
- ip ospf network, on page 417
- ip ospf priority, on page 417
- ip ospf retransmit-interval, on page 418

ip ospf area

To enable Open Shortest Path First version 2 (OSPFv2) on an interface, use the **ip ospf area** command in interface configuration mode. To disable OSPFv2 on the interface, use the **no** form of this command.

ip ospf *process-id* **area** *area-id*

no ip ospf *process-id* **area** [*area-id*]

Syntax Description

process-id	A decimal value in the range from 1 to 65535 that identifies the process ID.
area-id	A decimal value in the range from 0 to 4294967295, or an IP address in the dotted-decimal format.

Command Default

None

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For the usage guidelines, see ip ospf area.

Examples

```
Device(config)# interface GigabitEthernet 1
Device(config-if)# ip ospf 65535 area 1
```

ip ospf authentication

To specify the authentication type for an interface, use the **ip ospf authentication** command in interface or virtual network interface configuration mode. To remove the authentication for an interface, use the **no** form of this command.

ip ospf authentication message-digest
no ip ospf authentication

Syntax Description

message-digest	(Optional) Specifies that message-digest authentication is used.

Command Default

The authentication type for an interface is not configured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For the usage guidelines, see ip ospf authentication.

Examples

The following example shows how to enable message-digest authentication:

```
Device(config)# interface GigabitEthernet 1
Device (config-if)# ip ospf authentication message-digest
```

ip ospf cost

To explicitly specify the cost of sending a packet on an interface, use the **ip ospf cost** command in interface configuration mode. To reset the path cost to the default value, use the **no** form of this command.

ip ospf cost *interface-cost*
no ip ospf cost *interface-cost*

Syntax Description

interface-cost	Unsigned integer value expressed as the link-state metric. It can be a value in the range from 1 to 65535.

Command Default

No default cost is predefined.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For the usage guidelines, see ip ospf cost.

Examples

```
Device(config)# interface GigabitEthernet 1

Device(config-if)# ip ospf cost 65
```

ip ospf dead-interval

To set the interval during which at least one hello packet must be received from a neighbor before the router declares that neighbor down, use the **ip ospf dead-interval** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ip ospf dead-interval *seconds*
no ip ospf dead-interval

Syntax Description

seconds	Interval (in seconds) during which the router must receive at least one hello packet from a neighbor or else that neighbor is removed from the peer list and does not participate in routing. The range is 1 to 65535. The value must be the same for all nodes on the network.

Command Default

seconds : Four times the interval set by the **ip ospf hello-interval** command.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For the usage guidelines, see ip ospf dead-interval.

Examples

The following example sets the OSPF dead interval to 20 seconds:

```
Device(config)# interface GigabitEthernet 1
Device(config-if)# ip ospf dead-interval 20
```

ip ospf hello-interval

To specify the interval between hello packets that the Cisco IOS software sends on the interface, use the **ip ospf hello-interval** command in interface configuration mode. To return to the default time, use the **no** form of this command.

ip ospf hello-interval *seconds*

no ip ospf hello-interval

Syntax Description

seconds	Specifies the interval (in seconds). The value must be the same for all nodes on a specific network. The range is from 1 to 65535.

Command Default

10 seconds

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Qualified for use in Cisco vManage CLI templates.

Usage Guidelines

This value is advertised in the hello packets. The smaller the hello interval, the faster topological changes will be detected, but more routing traffic will ensue. This value must be the same for all routers and access servers on a specific network.

Examples

The following example sets the interval between hello packets to 15 seconds:

```
Device(config)# interface GigabitEthernet 1
Device(config-if)# ip ospf hello-interval 15
```

ip ospf message-digest-key md5

To enable Open Shortest Path First (OSPF) Message Digest 5 (MD5) authentication, use the **ip ospf message-digest-key md5**command in interface configuration mode. To remove an old MD5 key, use the **no** form of this command.

ip ospf message-digest-key *key-id* **md5** *key*
no ip ospf message-digest-key

Syntax Description

key-id	An identifier in the range from 1 to 255.
key	Alphanumeric password of up to 16 characters.

Command Default

OSPF MD5 authentication is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For the usage guidelines, see ip ospf message-digest-key md5.

Examples

```
Device(config)# interface GigabitEthernet 1
Device(config-if)# ip ospf message-digest-key 255 md5 7 00051105005E0D01072846
```

ip ospf network

To configure the Open Shortest Path First (OSPF) network type to a type other than the default for a given medium, use the **ip ospf network** command in interface configuration mode. To return to the default value, use the **no** form of this command.

ip ospf network broadcast
no ip ospf network

Syntax Description

broadcast	Sets the network type to broadcast.

Command Default

Depends on the network type.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For the usage guidelines, see ip ospf network.

Examples

The following example sets your OSPF network as a broadcast network:

```
Device(config)# interface GigabitEthernet 1
Device(config-if)# ip ospf network broadcast
```

ip ospf priority

To set the router priority, which helps determine the designated router for this network, use the **ip ospf priority** command in interface configuration mode. The priority is valid only for broadcast interfaces.

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

ip ospf priority *number-value*
noip ospf priority

Syntax Description

number-value	A number value that specifies the priority of the router. The range is from 0 to 255.

Command Default

Priority of 1

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For the usage guidelines, see ip ospf priority.

Examples

The following example sets the router priority value to 4:

```
Device(config)# interface GigabitEthernet 1
Device(config-if)# ip ospf priority 4
```

ip ospf retransmit-interval

To specify the time between link-state advertisement (LSA) retransmissions for adjacencies belonging to the interface, use the **ip ospf retransmit-interval** command in interface configuration mode. To return to the default value, use the **no** form of this command.

ip ospf retransmit-interval *seconds*
no ip ospf retransmit-interval

Syntax Description

seconds	Time (in seconds) between retransmissions. The range is from 1 to 65535 seconds. The default is 5 seconds.

Command Default

5 seconds

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Qualified for use in Cisco vManage CLI templates.

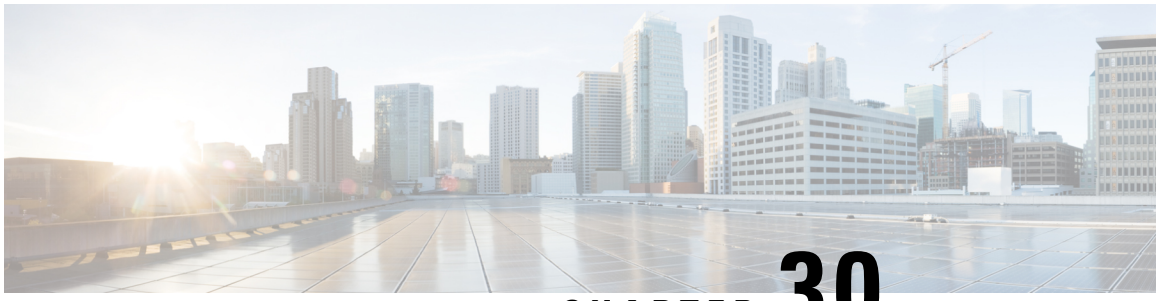
Usage Guidelines

For the usage guidelines, see ip ospf retransmit-interval.

Examples

The following example sets the retransmit interval value to 8 seconds:

```
Device(config)# interface GigabitEthernet 1
Device(config-if)# ip ospf retransmit-interval 8
```



CHAPTER 30

L2VPN Commands

- l2vpn sdwan instance, on page 419
- bridge-domain, on page 420
- l2protocol peer, on page 422
- l2protocol forward, on page 423

l2vpn sdwan instance

To configure an L2VPN instance on an Cisco IOS XE Catalyst SD-WAN device, use the **l2vpn sdwan instance** command in global configuration mode. To remove the configured L2VPN instance, use the **no** form of this command.

l2vpn sdwan instance *instance-id* { **multipoint** | **point-to-point** }

Syntax Description

instance-id	A unique number that identifies the VPN or VRF instance. It must be same on the edge devices participating in the Layer 2 domain. Range: 1 to 65531 **Note** Starting from Cisco IOS XE Catalyst SD-WAN Release 17.16.1a, the range is 1 to 511 and 513 to 65527.
multipoint	(Optional) Specifies multipoint as the instance type for connecting multiple sites within the same instance.
point-to-point	(Optional) Specifies point-to-point as the instance type for a direct connection between two edge devices.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.14.1a	This command was introduced.

Usage Guidelines

The instance ID must be a unique number. The ID must be the same on the Cisco IOS XE Catalyst SD-WAN devices participating in the Layer 2 domain. It must not overlap with your existing VRFs in the Cisco Catalyst SD-WAN fabric.

Examples

The following configures an L2VPN instance for point-to-point service:

```
Device(config)# l2vpn sdwan instance 10 point-to-point
```

The following configures an L2VPN instance for multipoint service:

```
Device(config)# l2vpn sdwan instance 20 multipoint
```

bridge-domain

To define a broadcast domain internal to a platform, use the **bridge-domain** command in global configuration mode. To remove the configured components from the bridge domain and to return the components to the bridge-domain default state, use the **no** form of this command.

bridge-domain *bridge-id*
member { *interface* **service-instance** *instance-id* | **sdwan-instance** *instance-id* [**remote-site-id** *site-id*] **vc-id** *vc-id* **single-homing** }

Syntax Description

bridge-domain *bridge-id*	Integer that identifies the bridge domain. Range: 1 to 16000 The upper limit may vary based on the platform.
member	The member interface specifies the LAN side interface or WAN side instance that participates in the bridge domain.
member *interface*	The LAN side interface that participates in the bridge domain.
member *interface* **service-instance**	Specifies the Ethernet service instance.
member *interface* **service-instance** *instance-id*	Specifies the ethernet service instance ID configured for the LAN interface. Range: 1 to 8000
member **sdwan-instance**	The sdwan-instance command is used to link the WAN side sdwan instance with the bridge-domain.

member **sdwan-instance** *instance-id*	Specifies the configured L2VPN SD-WAN instance ID. **Note** Starting from Cisco IOS XE Catalyst SD-WAN Release 17.16.1a, range is 1 to 511 and 513 to 65527.
instance-id	Specifies the ethernet service instance id configured under the LAN interface. It must be the same on the edge devices participating in the Layer 2 domain. Range: 1 to 65531
remote-site-id	The remote site id that participates in the P2P L2VPN sdwan instance.
site-id	Specifies the remote site ID. Range: 0 to 4294967295
vc-id	The Virtual Circuit (VC) ID that is used to identify a particular bridge domain.
vc-id	Specifies the Virtual Circuit (VC) ID. Range: 0 to 4294967295
single-homing	Specifies the homing type. Only single-homing is supported in Cisco IOS XE Catalyst SD-WAN Release 17.14.1a.
dual-homing	Specifies the homing type. Dual-homing is supported from Cisco IOS XE Catalyst SD-WAN Release 17.15.1a.

Command Default

Bridging is disabled.

Command Modes

Global configuration (config) and bridge-domain config

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.14.1a	The command was introduced.
Cisco IOS XE Catalyst SD-WAN Release 17.15.1a	Added **dual-homing** keyword.

Usage Guidelines

Use the command to link LAN side interface with bridge-domain. Enter the bridge-domain configuration mode, then enter the member commands.

Examples

The following example shows a bridge-domain 30 and service instance ID 20 configured for P2P connection and bridge-domain 31 with service instance ID 21 for P2MP connection for an edge device in a site using single-homing:

```
Device(config)# bridge-domain 30
Device(config-bdomain)# member GigabitEthernet7 service-instance 20
Device(config-bdomain-efp)# member sdwan-instance 10  remote-site 2 vc-id 1 single-homing
Device(config-bdomain)# exit
```

```
Device(config)# bridge-domain 31
Device(config-bdomain)# member GigabitEthernet7 service-instance 21
Device(config-bdomain-efp)# member sdwan-instance 11 vc-id 1 single-homing
```

The following example shows a bridge-domain 10 and service instance ID 20 configured for P2P connection and bridge-domain 20 with service instance ID 21 for P2MP connection for an edge device in a site using dual-homing:

```
Device(config)# bridge-domain 10
Device(config-bdomain)# member GigabitEthernet7 service-instance 20
Device(config-bdomain-efp)# member sdwan-instance 10  remote-site 2 vc-id 1 dual-homing
Device(config-bdomain)# exit
Device(config)# bridge-domain 20
Device(config-bdomain)# member GigabitEthernet7 service-instance 21
Device(config-bdomain-efp)# member sdwan-instance 11 vc-id 1 dual-homing
```

l2protocol peer

To enable Layer 2 packets peer for supported Layer 2 control protocols (such as STP, CDP, VTP, or others) on a specific SD-WAN instance, use the **l2protocol peer** command in interface configuration mode. To disable Layer 2 packets peer processing, use the **no** form of this command.

l2protocol peer { **R4** | **R5** | **R6** | **R8** | **R9** | **RA** | **RB** | **RC** | **RD** | **RF** | **cdp** | **dot1x** | **dtp** | **elmi** | **esmc** | **lacp** | **lldp** | **pagp** | **ptppd** | **stp** | **udld** | **vtp** }

no l2protocol peer { **R4** | **R5** | **R6** | **R8** | **R9** | **RA** | **RB** | **RC** | **RD** | **RF** | **cdp** | **dot1x** | **dtp** | **elmi** | **esmc** | **lacp** | **lldp** | **pagp** | **ptppd** | **stp** | **udld** | **vtp** }

Syntax Description

R4	Reserved Protocol using destination Mac 0180.C200.0004
R5	Reserved Protocol using destination Mac 0180.C200.0005
R6	Reserved Protocol using destination Mac 0180.C200.0006
R8	Reserved Protocol using destination Mac 0180.C200.0008
R9	Reserved Protocol using destination Mac 0180.C200.0009
RA	Reserved Protocol using destination Mac 0180.C200.000A
RB	Reserved Protocol using destination Mac 0180.C200.000B
RC	Reserved Protocol using destination Mac 0180.C200.000C
RD	Reserved Protocol using destination Mac 0180.C200.000D
RF	Reserved Protocol using destination Mac 0180.C200.000F
cdp	Cisco Discovery Protocol
dot1x	802.1x Protocol
dtp	Dynamic Trunking Protocol

elmi	ELMI Protocol
esmc	ESMC Protocol
lacp	LACP Protocol
lldp	Link Layer Discovery Protocol
pagp	Port Aggregation Protocol
ptppd	PTP Peer Delay Protocol
stp	Spanning Tree Protocol
udld	UDLD Protocol
vtp	VLAN Trunking Protocol

Command Default

None

Command Modes

Global configuration (config) and l2sdwan sdi config

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.18.1a	The command was introduced.

Usage Guidelines

Use the command in P2P mode to control the Control Protocol (L2CP) packets you want to block or use locally. Enter the P2P mode to block L2CP packets, then enter the **l2protocol peer** commands.

Examples

The example shows a l2vpn sdwan instance 222 point-to-point configuration. In the example, SD-WAN instance 222 will no longer forward Cisco Discovery Protocol (CDP) and Spanning Tree Protocol (STP). packets.

```
Device(config)# l2vpn sdwan instance 222 point-to-point
Device(config-l2sdwan-sdi)# l2protocol peer cdp stp
Device(config-l2sdwan-sdi)# exit
Device(config)# exit
```

l2protocol forward

To enable the forwarding of Layer 2 protocol packets on specific SD-WAN instance in a multipoint setup, use the **l2protocol forward** command in interface configuration mode. To disable Layer 2 protocol packet forwarding on the interface, use the **no** form of this command.

l2protocol forward { **R4** | **R5** | **R6** | **R8** | **R9** | **RA** | **RB** | **RC** | **RD** | **RF** | **cdp** | **dot1x** | **dtp** | **elmi** | **esmc** | **lacp** | **lldp** | **pagp** | **ptppd** | **stp** | **udld** | **vtp** }

no l2protocol forward { **R4** | **R5** | **R6** | **R8** | **R9** | **RA** | **RB** | **RC** | **RD** | **RF** | **cdp** | **dot1x** | **dtp** | **elmi** | **esmc** | **lacp** | **lldp** | **pagp** | **ptppd** | **stp** | **udld** | **vtp** }

Syntax Description

R4	Reserved Protocol using destination Mac 0180.C200.0004
R5	Reserved Protocol using destination Mac 0180.C200.0005
R6	Reserved Protocol using destination Mac 0180.C200.0006
R8	Reserved Protocol using destination Mac 0180.C200.0008
R9	Reserved Protocol using destination Mac 0180.C200.0009
RA	Reserved Protocol using destination Mac 0180.C200.000A
RB	Reserved Protocol using destination Mac 0180.C200.000B
RC	Reserved Protocol using destination Mac 0180.C200.000C
RD	Reserved Protocol using destination Mac 0180.C200.000D
RF	Reserved Protocol using destination Mac 0180.C200.000F
cdp	Cisco Discovery Protocol
dot1x	802.1x Protocol
dtp	Dynamic Trunking Protocol
elmi	ELMI Protocol
esmc	ESMC Protocol
lacp	LACP Protocol
lldp	Link Layer Discovery Protocol
pagp	Port Aggregation Protocol
ptppd	PTP Peer Delay Protocol
stp	Spanning Tree Protocol
udld	UDLD Protocol
vtp	VLAN Trunking Protocol

Command Default

None

Command Modes

Global configuration (config) and l2sdwan sdi config

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.18.1a	The command was introduced.

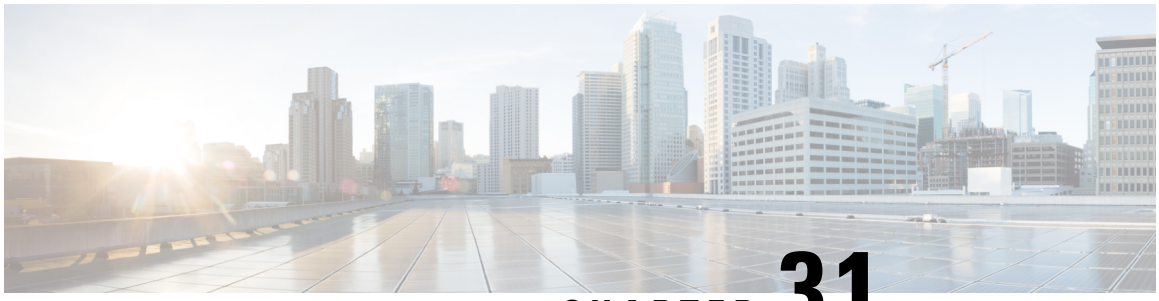
Usage Guidelines

Use the command to configure the SD-WAN instance to forward Layer 2 protocol packets, allowing protocol transparency across a Layer 2 VPN or tunneling environment. Enter the multipoint modes to forward l2cp packets, then enter the **l2protocol forward** commands.

Examples

This example shows the l2vpn sdwan instance 111 multipoint configurations. In the example, SD-WAN instance 111 actively forwards Cisco Discovery Protocol (CDP) and Spanning Tree Protocol (STP) packets. This implies that these packets are transparently passed through the L2VPN to the remote endpoints.

```
Device(config)# l2vpn sdwan instance 111 multipoint
Device(config-l2sdwan-sdi)# l2protocol forward cdp stp
```



CHAPTER 31

LAN Switching Commands

- spanning-tree bpduguard, on page 427
- spanning-tree guard, on page 427
- spanning-tree mode, on page 428
- spanning-tree portfast (interface), on page 428

spanning-tree bpduguard

To enable bridge protocol data unit (BPDU) guard on the interface, use the **spanning-tree bpduguard** command in interface configuration and template configuration mode. To return to the default settings, use the **no** form of this command.

Supported Parameters

enable	Enables BPDU guard on this interface.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE spanning-tree bpduguard command.

Examples

```
spanning-tree guard root
spanning-tree bpduguard enable
```

spanning-tree guard

To enable or disable the guard mode, use the **spanning-tree guard** command in interface configuration and template configuration mode. To return to the default settings, use the **no** form of this command.

Supported Parameters

root	Enables root-guard mode on the interface.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE spanning-tree guard command.

Examples

```
spanning-tree guard root
spanning-tree bpduguard enable
```

spanning-tree mode

To switch between Per-VLAN Spanning Tree+ (PVST+), Rapid-PVST+, and Multiple Spanning Tree (MST) modes, use the **spanning-treemode** command in global configuration mode. To return to the default settings, use the **no** form of this command.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates. The command option **rapid-pvst** is qualified.

Usage Guidelines

For more information about this command, see the Cisco IOS XE `spanning-tree mode` command.

Examples

```
Device# config-transaction
Device(config)# spanning-tree mode rapid-pvst
```

spanning-tree portfast (interface)

To enable PortFast mode where the interface is immediately put into the forwarding state upon linkup without waiting for the timer to expire, use the **spanning-treeportfast** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

Command History

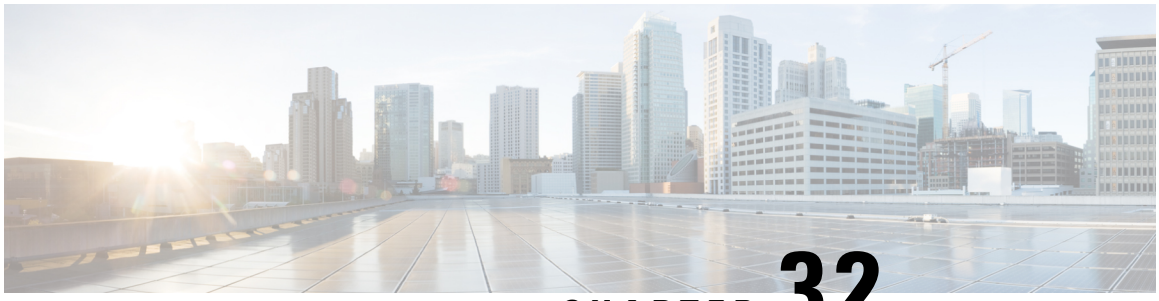
Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE `spanning-tree portfast (interface)` command.

Examples

```
Device(config-if)# spanning-tree portfast
```



CHAPTER 32

Line Commands

- exec-timeout, on page 431
- ip telnet disable, on page 432
- line, on page 433
- line con transport, on page 434
- line vty transport, on page 435
- line aux transport, on page 437
- password (line configuration), on page 438
- privilege level, on page 439

exec-timeout

To set the interval that the EXEC command interpreter waits until user input is detected, use the **exec-timeout** command in line configuration mode. To remove the timeout definition, use the **no** form of this command.

exec-timeout *minutes* [*seconds*]
no exec-timeout

Syntax Description

minutes	Integer that specifies the number of minutes. The default is 10 minutes.
seconds	(Optional) Additional time intervals in seconds.

Command Default

10 minutes

Command Modes

Line configuration (config-line)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	This command was introduced.

Usage Guidelines

If no input is detected during the interval, the EXEC facility resumes the current connection. If no connections exist, the EXEC facility returns the terminal to the idle state and disconnects the incoming session.

To specify no timeout, enter the **no** form of this command.

Examples

The following example shows how to set a time interval of 2 minutes, 30 seconds:

```
Device(config)# line console 0
Device(config-line)# exec-timeout 2 30
```

The following example shows how to set a time interval of 10 seconds:

```
Device(config)# line aux 0
Device(config-line)# exec-timeout 0 10
```

ip telnet disable

To disable Telnet access on IOS-XE devices, SD-WAN, SD-Routing, and autonomous platforms, use the **ip telnet disable** command in the global configuration mode. To restore telnet access, a configuration reset is required.

ip telnet disable

Restore telnet access

If	Then
Autonomous and SD-Routing	**factory-reset all** or **controller-mode reset** or **write erase**
SD-WAN	**request platform software sdwan config reset** **request platform software sdwan software reset** **controller-mode reset**

Command Default

Telnet access is enabled

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.18.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Use the **ip telnet disable** command when you need to permanently restrict Telnet access to the device, as this action cannot be easily reversed.

line

To identify a specific line for configuration and enter line configuration collection mode, use the **line** command in global configuration mode. To remove configuration from a specific line, use the **no** form of this command.

line { **auto-consolidation** | **aux** | **con 0** | **range** | **vty** *line-number* }
no line { **auto-consolidation aux** | **con 0** | **range** | **vty** *line-number* }

auto-consolidation	Enable or disable auto-consolidation of terminal lines.
aux	(Optional) Auxiliary EIA/TIA-232 DTE port. Must be addressed as relative line 0. The auxiliary port can be used for modem support and asynchronous connections.
con 0	Console 0 terminal line. The console port is DCE.
vty	Virtual terminal line for remote console access.
range	Range of lines with first line number and last line number.
line-number	Relative number of the virtual terminal line (or the first line in a contiguous group) that you want to configure when the line type is specified. Numbering begins with zero. You can either configure a single line or a range.

Command Default

There is no default line.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	Additional parameters qualified: **auto-consolidation**, **aux** and **range**.
Cisco IOS XE Catalyst SD-WAN Release 26.2.1	**aux** parameter is not supported.

Usage Guidelines

From Cisco IOS XE Catalyst SD-WAN Release 26.2.1, **aux** parameter is unsupported. During an upgrade, SD-WAN Manager handles this command automatically.

For usage guidelines, see the Cisco IOS line command.

Examples

The terminal from which you locally configure the router is attached to the console port. To configure line parameters for the console port, enter the following:

```
line console 0
```

The following example starts configuration for virtual terminal lines 0 to 4:

```
line vty 0 4
```

The following example configuration shows how to disable auto-consolidation:

```
line auto-consolidation
```

To configure line parameters for the auxiliary port, enter the following:

```
line aux 0
```

The following example starts configuration for a range of lines:

```
line range 1 5
```

line con transport

To set transport output parameters for line console 0, use the **transport** command in line console 0 configuration mode. To remove transport parameters for line console 0, use the **no** form of this command.

transport { **output** [*aceron* | *all* | *lapb-ta* | *lat* | *mop* | *nasi* | *none* | *pad* | *rlogin* | *ssh* | *telnet* | *udptn* | *v120*] }
no transport { **output** [*aceron* | *all* | *lapb-ta* | *lat* | *mop* | *nasi* | *none* | *pad* | *rlogin* | *ssh* | *telnet* | *udptn* | *v120*] }

Table 28: Syntax Description

output	Defines the protocols that can be used from outgoing connections line.
aceron	(Optional) Selects the remote console for Application Control Engine (ACE)-based blade.
all	Assigns the device or interface as the designated-gateway for the domain.
lapb-ta	(Optional) Selects the ISDN link access procedure, balanced-terminal adapter protocol.
lat	(Optional) Selects the digital local-area transport (LAT) protocol and specifies both incoming reverse LAT and host-initiated connections.
mop	(Optional) Selects Maintenance Operation Protocol (MOP).
nasi	(Optional) Selects NetWare Access Servers Interface (NASI) as the input transport protocol.
none	Prevents any protocol selection on the line. This makes the port unusable by incoming connections.
pad	(Optional) Selects X.3 packet assembler/disassembler (PAD) incoming connections.
rlogin	(Optional) Selects the UNIX rlogin protocol.
ssh	(Optional) Selects the Secure Shell (SSH) protocol.

telnet	(Optional) Specifies all types of incoming TCP/IP connections.
udptn	(Optional) Specifies the asynchronous data that is sent through UDP Telnet (UDPTN).
v120	(Optional) Selects the v120 protocol for incoming asynchronous connections over ISDN.

Command Default

SSH is enabled for incoming connections by default on VTY lines only.

Command Modes

Line console configuration (config-line).

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

You can specify one protocol, multiple protocols, all protocols, or no protocols. To specify multiple protocols, enter the keyword for each protocol, separated by a space under any line configuration mode.

Examples

The following example shows how to configure the line console 0 to only allow ssh connections from the console 0 interface.

```
Device(config)# line console 0
Device(config-line)# transport output ssh
```

line vty transport

To set transport input and output parameters for line vty 0 4, use the **transport** command in line vty 0 4 configuration mode. To remove transport parameters for line vty 0 4, use the **no** form of this command.

transport { **input** [*aceron* | *all* | *lapb-ta* | *lat* | *mop* | *nasi* | *none* | *pad* | *rlogin* | *ssh* | *telnet* | *udptn* | *v120*] | **output** [*aceron* | *all* | *lapb-ta* | *lat* | *mop* | *nasi* | *none* | *pad* | *rlogin* | *ssh* | *telnet* | *udptn* | *v120*] }
no transport { **input** [*aceron* | *all* | *lapb-ta* | *lat* | *mop* | *nasi* | *none* | *pad* | *rlogin* | *ssh* | *telnet* | *udptn* | *v120*] | **output** [*aceron* | *all* | *lapb-ta* | *lat* | *mop* | *nasi* | *none* | *pad* | *rlogin* | *ssh* | *telnet* | *udptn* | *v120*] }

Table 29: Syntax Description

input	Defines the protocols to be used to connect to a specific line of the router.
output	Defines the protocols that can be used for outgoing connections from line.

aceron	(Optional) Selects the remote console for Application Control Engine (ACE)-based blade.
all	Assigns the device or interface as the designated-gateway for the domain.
lapb-ta	(Optional) Selects the ISDN link access procedure, balanced-terminal adapter protocol.
lat	(Optional) Selects the digital local-area transport (LAT) protocol and specifies both incoming reverse LAT and host-initiated connections.
mop	(Optional) Selects Maintenance Operation Protocol (MOP).
nasi	(Optional) Selects NetWare Access Servers Interface (NASI) as the input transport protocol.
none	Prevents any protocol selection on the line. This makes the port unusable by incoming connections.
pad	(Optional) Selects X.3 packet assembler/disassembler (PAD) incoming connections.
rlogin	(Optional) Selects the UNIX rlogin protocol.
ssh	(Optional) Selects the Secure Shell (SSH) protocol.
telnet	(Optional) Specifies all types of incoming TCP/IP connections.
udptn	(Optional) Specifies the asynchronous data that is sent through UDP Telnet (UDPTN).
v120	(Optional) Selects the v120 protocol for incoming asynchronous connections over ISDN.

Command Default

SSH is enabled for incoming connections on VTY lines.

Command Modes

Line VTY configuration (config-line).

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

You can specify one protocol, multiple protocols, all protocols, or no protocols. To specify multiple protocols, enter the keyword for each protocol, separated by a space under any line configuration mode.

Examples

The following example shows how to configure the line vty 0 4 to only allow ssh connections.

```
Device(config)#line vty 0 4
Device(config-line)#transport input ssh
```

line aux transport

To define which protocols to use to connect to a specific line of the router, use the **transport input** command in line configuration mode. To change or remove the protocol, use the **no** form of this command.

transport { **input** [*aceron* | *all* | *lat* | *mop* | *nasi* | *none* | *pad* | *rlogin* | *ssh* | *telnet* | *udptn* | *v120*] | **output** [*aceron* | *all* | *lapb-ta* | *lat* | *mop* | *nasi* | *none* | *pad* | *rlogin* | *ssh* | *telnet* | *udptn* | *v120*] }
no transport { **input** [*aceron* | *all* | *lat* | *mop* | *nasi* | *none* | *pad* | *rlogin* | *ssh* | *telnet* | *udptn* | *v120*] | **output** [*aceron* | *all* | *lapb-ta* | *lat* | *mop* | *nasi* | *none* | *pad* | *rlogin* | *ssh* | *telnet* | *udptn* | *v120*] }

Table 30: Syntax Description

input	Defines the protocols to be used to connect to a specific line of the router.
output	Defines the protocols that can be used for outgoing connections from line.
aceron	(Optional) Selects the remote console for Application Control Engine (ACE)-based blade.
all	Assigns the device or interface as the designated-gateway for the domain.
lat	(Optional) Selects the digital local-area transport (LAT) protocol and specifies both incoming reverse LAT and host-initiated connections.
mop	(Optional) Selects Maintenance Operation Protocol (MOP).
nasi	(Optional) Selects NetWare Access Servers Interface (NASI) as the input transport protocol.
none	Prevents any protocol selection on the line. This makes the port unusable by incoming connections.
pad	(Optional) Selects X.3 packet assembler/disassembler (PAD) incoming connections.
rlogin	(Optional) Selects the UNIX rlogin protocol.
ssh	(Optional) Selects the Secure Shell (SSH) protocol.

telnet	(Optional) Specifies all types of incoming TCP/IP connections.
udptn	(Optional) Specifies the asynchronous data that is sent through UDP Telnet (UDPTN).
v120	(Optional) Selects the v120 protocol for incoming asynchronous connections over ISDN.

Command Default No protocols are allowed on the auxiliary (AUX) lines.

Command Modes Line configuration (config-line)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	This command was introduced.

Usage Guidelines You can specify one protocol, multiple protocols, all protocols, or no protocols. To specify multiple protocols, enter the keyword for each protocol, separated by a space under any line configuration mode.

The following example shows how to set the incoming protocol for the aux line 0 to Telnet:

```
Device(config)# line aux 0
Device(config-line)# exec-timeout 0 10
Device(config-line)# transport input
```

password (line configuration)

To specify a password on a line, use the **password** command in line configuration mode. To remove the password, use the **no** form of this command.

password *password*
no password

Syntax Description

password	Character string that specifies the line password. The first character cannot be a number. The string can contain any alphanumeric characters, including spaces, up to 80 characters. You cannot specify the password in the format number-space-anything. The space after the number causes problems. For example, hello 21 is a legal password, but 21 hello is not. The password checking is case sensitive. For example, the password Secret is different than the password secret.

Command Default No password is specified.

Command Modes Line configuration (config-line)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE password command.

Examples

The following example removes the password from virtual terminal lines 1 to 4:

```
Device(config)# line vty 1 4
Device(config-line)# no password
```

The following example removes the password from aux line 0:

```
Device(config)# line aux 0
Device(config-line)# no password
```

privilege level

To set the default privilege level for a line, use the **privilege level** command in line configuration mode. To restore the default user privilege level to the line, use the **no** form of this command.

privilege level *level*
no privilege level

Syntax Description

level	Privilege level associated with the specified line.

Command Default

Level 15 is the level of access permitted by the enable password.

Level 1 is normal EXEC-mode user privileges.

Command Modes

Line configuration (config-line)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	This command was introduced.

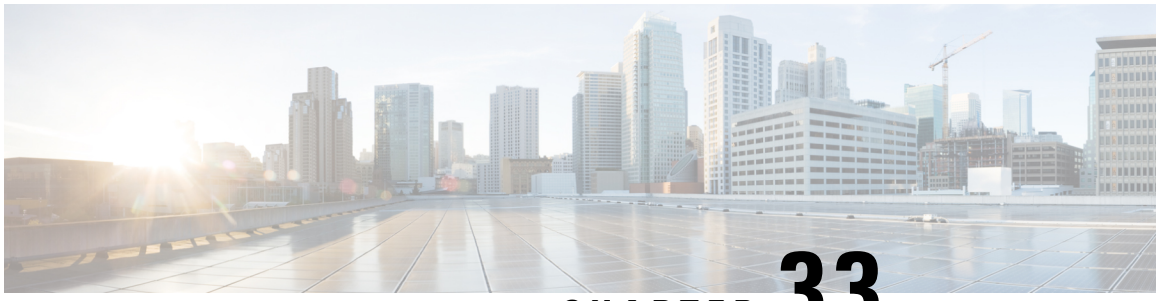
Usage Guidelines

For usage guidelines, see the Cisco IOS XE privilege level command.

Examples

The following example shows how to configure the auxiliary line for privilege level 5. Anyone using the auxiliary line has privilege level 5 by default:

```
Device(config)# line aux 0
Device(config-line)# privilege level 5
```



CHAPTER 33

Logging Commands

- banner login, on page 441
- logging buffered, on page 442
- logging console, on page 443
- logging discriminator, on page 443
- logging host, on page 445
- logging monitor, on page 446
- logging persistent, on page 446
- logging rate-limit, on page 447
- logging source-interface, on page 448
- logging tls-profile ciphersuite, on page 448
- logging tls-profile tls-version, on page 450
- logging trap, on page 450
- logging trap informational syslog-format rfc5424, on page 451
- service timestamps, on page 452

banner login

To define and enable a customized banner to be displayed before the username and password login prompts, use the **banner login** command in global configuration mode. To disable the login banner, use **no** form of this command.

banner login *message*
no banner login

Command Default

Disabled (no login banner is displayed).

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE 17.3.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

To configure multi-line banner use \\x0a as newline character. For usage guidelines, see the Cisco IOS XE banner login command.

Examples

The following example sets a login banner.

```
Device# banner login Access for authorized users only. Please enter your username and
password.


Device#show banner login
Access for authorized users only. Please enter your username and password.
Device#
```

logging buffered

To enable system message logging to a local buffer, use the **logging buffered** command in global configuration mode. To cancel the use of the buffer, use the **no** form of this command. To return the buffer size to its default value, use the **default** form of this command.

logging buffered *buffer-size*
no logging buffered
default logging buffered

Syntax Description

buffer-size	Size of the buffer, in bytes. The range is 4096 to 2147483647. The default size varies by platform.

Command Default

Varies by platform. For most platforms, logging to the buffer is disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE logging buffered command.

Examples

The following example shows how to enable standard system logging to the local syslog buffer:

```
Router(config)# logging buffered
```

logging console

To send system logging (syslog) messages to all available TTY lines and limit messages based on severity, use the **logging console** command in global configuration mode. To disable logging to the console terminal, use the **no** form of this command.

logging console
no logging console

Command Default

The default varies by platform. In general, the default is to log all messages.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE logging console command.

Examples

The following is an example for this command:

```
Router(config)# logging console
```

logging discriminator

To create a syslog message discriminator, use the **logging discriminator** command in global configuration mode. To disable the syslog message discriminator, use the **no** form of this command.

logging discriminator *discr-name* [[**facility**] [**mnemonics**] [**msg-body**] { **drops** *string* | **includes** *string* }] [**severity** { **drops** *sev-num* | **includes** *sev-num* }] [**rate-limit** *msglimit*]
no logging discriminator *discr-name*

Syntax Description

discr-name	String of a maximum of eight alphanumeric, case-sensitive characters. Blank spaces between characters are not allowed.
facility	(Optional) Message subfilter for the facility pattern in an event message.
mnemonics	(Optional) Message subfilter for the mnemonic pattern in an event message.
msg-body	(Optional) Message subfilter for the msg-body pattern in an event message.
drops	Drops messages that match the pattern, including the specified regular expression.
includes	Delivers messages that match the pattern, including the specified regular expression string.

string	(Optional) Expression used for message filtering.
severity	(Optional) Message subfilter by severity level or group.
sev-num	(Optional) Integer that identifies the severity level or multiple levels. Multiple levels must be separated with a comma (,).
rate-limit	(Optional) Specifies a number of messages to be processed within a unit of time.
msglimit	(Optional) Integer in the range of 1 to 10000 that identifies the number of messages not to be exceeded.

Command Default

The logging discriminator function is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	This command was introduced.

Usage Guidelines

If you enter a discriminator name that was previously specified, your entry is treated as a modification to the discriminator. The modification becomes effective when the configuration is completed. All associated sessions will use the modified value. When you remove a discriminator, the associations of all entries in the logging host list are removed.

When you issue the**no logging discriminator** command and the discriminator name is not found, an error message is generated. If the discriminator name is valid and actively associated with syslog sessions, the effect is immediate; the next syslog message to be processed will go through.

Subfilters are checked in the following order. If a message is dropped by any of the subfilters, the remaining checks are skipped.

1. Severity level or levels specified
2. Facility within the message body that matches a regular expression
3. Mnemonic that matches a regular expression
4. Part of the body of a message that matches a regular expression
5. Rate-limit

Examples

The following example shows how to enable the logging discriminator named msglog01 to filter messages with a severity level of 5.

```
Device(config)# logging discriminator msglog01 severity includes 5
```

logging host

To log system messages and debug output to a remote host, use the **logging host** command in global configuration mode. To remove a specified logging host from the configuration, use the **no** form of this command.

logging host { [*ip-address*] [**vrf** *vrf-value*] | [**discriminator** *discr-name*] }

Syntax Description

ip-address	(Optional) IP address of the host that will receive the system logging (syslog) messages.
vrf *vrf-value*	(Optional) Specifies a VPN routing and forwarding instance (VRF) that connects to the syslog server host.
discriminator *discr-name*	(Optional) Specifies a message discriminator for the session. Name of the message discriminator.

Command Default

System logging messages are not sent to any remote host.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE logging host command.

Note Creating and deleting the logging host configurations in same transaction causes unexpected behaviour. For example, deleting **logging host** *ipv4-address* and creating **logging host** *ipv4-address* **vrf** *vrf-name* configuration in same transaction causes both configurations to disappear from the device. We recommend you to send the two requests in separate transactions.

Examples

In the following example, messages are logged to a host with an IP address of 172.16.150.63 connected through a VRF:

```
Device(config)# logging host 172.16.150.63 vrf 4

exit
Device(config)# logging host 172.16.150.63 vrf 4 discriminator discr1

exit
```

logging monitor

To enable system message logging to the terminal lines (monitor connections), use the **logging console** command in global configuration mode. To disable all logging to the monitor connections, use the **no** form of this command.

logging monitor
no logging monitor

Command Default

Logging to monitor connections is enabled.

The default severity level varies by platform, but is generally level 7 (messages at levels 0 through 7 are logged).

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE logging monitor command.

Examples

In the following example, the user enables system message logging to the console for messages:

```
Router(config)# logging monitor
```

logging persistent

To enable the storage of logging messages on the router's advanced technology attachment (ATA) disk, use the **logging persistent** command in global configuration mode. To disable logging message storage on the ATA disk, use the **no** form of this command.

logging persistent { **filesize** *logging-file-size* } { **size** *filesystem-size* }
no logging persistent

Syntax Description

filesize *logging-file-size*	(Optional) Specifies the size of individual logging files in bytes. • Minimum value is 8192. • Maximum value is 2147483647. • Default value is 262144.

size *filesystem-size*	(Optional) Specifies the amount of disk space, in bytes, allocated to syslog messages. • Minimum value is 16384. • Maximum value is 2147483647. • Default value is 10 percent of the total disk space.

Command Default

The logging messages are not stored in the router's ATA memory.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE logging persistent command.

Examples

The following is an example:

```
Router> enable
Router# configure terminal
Router(config)# logging persistent size 104857600 filesize 10485760
Router(config)# exit
```

logging rate-limit

To limit the rate of messages logged per second, use the **logging rate-limit** command in global configuration mode . To disable the limit, use the **no** form of this command.

logging rate-limit
no logging rate-limit

Command Default

The default is 10 messages logged per second.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE logging rate-limit command.

Examples

The following is an example of this command:

```
Router(config)# logging rate-limit
```

logging source-interface

To specify the source IPv4 or IPv6 address of system logging packets, use the **logging source-interface** command in global configuration mode. To remove the source designation, use the **no** form of this command.

logging source-interface [**interface-name** *number* **vrf** *vrf-name*]
no logging source-interface [**interface-name** *number* **vrf** *vrf-name*]

Syntax Description

Interface-name *number*	Interface type and number.
vrf *vrf-name*	Provides logging source-interface setting capability to Virtual Routing and Forwarding (VRF) syslog destinations. Name assigned to the VRF.

Command Default

The wildcard interface address is used.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE logging source-interface command.

Examples

The following example shows how to specify that the IP address of Ethernet interface 0 as the source IP address for all syslog messages:

```
Router(config)# logging source-interface loopback111 vrf4
```

logging tls-profile ciphersuite

To set the cipher suite for logging tls-profiles, use the **logging tls-profile ciphersuite** command in global configuration mode. To remove the cipher suite, use the **no** form of this command.

logging tls-profile *name* **ciphersuite** { **aes-128-cbc-sha** | **aes-256-cbc-sha** | **dhe-aes-cbc-sha2** | **dhe-aes-gcm-sha2** | **ecdhe-ecdsa-aes-gcm-sha2** | **ecdhe-rsa-aes-cbc-sha2** | **ecdhe-rsa-aes-gcm-sha2** | **rsa-aes-cbc-sha2** | **rsa-aes-gcm-sha2** }
no logging tls-profile *name* **ciphersuite** { **aes-128-cbc-sha** | **aes-256-cbc-sha** | **dhe-aes-cbc-sha2** | **dhe-aes-gcm-sha2** | **ecdhe-ecdsa-aes-gcm-sha2** | **ecdhe-rsa-aes-cbc-sha2** | **ecdhe-rsa-aes-gcm-sha2** | **rsa-aes-cbc-sha2** | **rsa-aes-gcm-sha2** }

Syntax Description

name	Name of existing or new logging tls-profile.
aes-128-cbc-sha	Specifies the ciphersuite to aes-128-cbc-sha.
aes-256-cbc-sha	Specifies the ciphersuite to aes-256-cbc-sha.
dhe-aes-cbc-sha2	Specifies the ciphersuite to dhe-aes-cbc-sha2.
dhe-aes-gcm-sha2	Specifies the ciphersuite to dhe-aes-gcm-sha2.
ecdhe-ecdsa-aes-gcm-sha2	Specifies the ciphersuite to ecdhe-ecdsa-aes-gcm-sha2.
ecdhe-rsa-aes-cbc-sha2	Specifies the ciphersuite to ecdhe-rsa-aes-cbc-sha2.
ecdhe-rsa-aes-gcm-sha2	Specifies the ciphersuite to ecdhe-rsa-aes-gcm-sha2.
rsa-aes-cbc-sha2	Specifies the ciphersuite to rsa-aes-cbc-sha2.
rsa-aes-gcm-sha2	Specifies the ciphersuite to rsa-aes-gcm-sha2.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Cisco IOS XE Catalyst SD-WAN devices now support sending secure syslog messages over the Transport Layer Security (TLS) as per RFC5425. To secure the syslog message content from potential tampering, the TLS protocol is used for certificate exchange, mutual authentication, and ciphers negotiation. Use this **logging tls-profile ciphersuite** command to set the cipher suite of the logging tls-profile.

Example

The following example shows how to set the cipher suite of profile1 to aes-256-cbc-sha.

```
Device(config)# logging tls-profile profile1 ciphersuite aes-256-cbc-sha
```

Table 31: Related Commands

Command	Description
tls-version	Specifies the TLS version.
client-id-trustpoint	Specifies the client ID trustpoint.

logging tls-profile tls-version

To set the tls-version for logging tls-profiles, use the **logging tls-profile tls-version** command in global configuration mode. To remove the tls-version, use the **no** form of this command.

logging tls-profile *name* **tls-version** { **TLSv1.1** | **TLSv1.2** }
no logging tls-profile *name* **tls-version**

Syntax Description

name	Name of logging tls-profile.
TLSv1.1	Specifies TLSv1.1 as the version to be used.
TLSv1.2	Specifies TLSv1.2 as the version to be used.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Cisco IOS XE Catalyst SD-WAN devices now support sending secure syslog messages over Transport Layer Security (TLS) as per RFC5425. To secure the syslog message content from potential tampering, the TLS protocol is used for certificate exchange, mutual authentication, and ciphers negotiation. Use this **logging tls-profile tls-version** command to set the tls-version of the logging tls-profile to TLSv1.1 or TLSv1.2.

Example

The following example shows how to set the tls-version of profile1 to TLSv1.1.

```
Device(config)# logging tls-profile profile1 tls-version TLSv1.1
```

Table 32: Related Commands

Command	Description
ciphersuite	Specifies the cipher suite.
client-id-trustpoint	Specifies the client ID trustpoint.

logging trap

To limit messages logged to the syslog servers based on severity, use the **logging trap** command in global configuration mode . To return the logging to remote hosts to the default level, use the **no** form of this command.

logging trap { [**errors**] }
no logging trap

Command Default

Syslog messages at level 0 to level 6 are generated, but will only be sent to a remote host if the **logging host** command is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE logging trap command.

Examples

In the following is an example for this command:

```
Router(config)# logging trap error
```

logging trap informational syslog-format rfc5424

To set the logging trap level to informational and the syslog format to rfc5424, use the **logging trap informational syslog-format rfc5424** command in global configuration mode. To remove the logging trap informational syslog-format rfc5424, use the **no** form of this command.

logging trap informational syslog-format rfc5424
no logging trap informational syslog-format rfc5424

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

There are various severity levels of message logging. Specifying a level causes messages at that level and numerically lower levels to be displayed at the destination. There are two syslog formats - RFC3164 and RFC5424. Use this **logging trap informational syslog-format rfc5424** command to set the logging trap level to informational and the syslog format to rfc5424.

Example

The following example shows how to set the trap level to informational and syslog format to rfc5424.

```
Device(config)# logging trap informational syslog-format rfc5424
```

service timestamps

To configure the system to apply a time stamp to debugging messages or system logging messages, use the **service timestamps** command in global configuration mode. To disable this service, use the **no** form of this command.

service timestamps [**debug** | **log**] { **datetime** } [**msec** | **localtime** | **show-timezone** | **year**]
no service timestamps [**debug** | **log**]

Syntax Description

debug	(Optional) Indicates time-stamping for debugging messages.
log	(Optional) Indicates time-stamping for system logging messages.
datetime	(Optional) Specifies that the time stamp should consist of the date and time. • The time-stamp format for **datetime** is MMM DD HH:MM:SS, where MMM is the month, DD is the date, HH is the hour (in 24-hour notation), MM is the minute, and SS is the second. • If the datetime keyword is specified, you can optionally add the **msec**, **localtime**, **show-timezone**, or **year** keywords. • If the **service timestamps datetime** command is used without addtional keywords, time stamps will be shown using UTC, without the year, without milliseconds, and without a time zone name.
msec	(Optional) Includes milliseconds in the time stamp, in the format HH: DD: MM: SS. mmm, where .mmm is milliseconds.
localtime	(Optional) Time stamp relative to the local time zone.
year	(Optional) Include the year in the date-time format.
show-timezone	(Optional) Include the time zone name in the time stamp. **Note** If the localtime keyword option is not used (or if the local time zone has not been configured using the **clock timezone** command), time will be displayed in Coordinated Universal Time (UTC).

Command Default

Time stamps are applied to debug and logging messages.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE service timestamps command.

Examples

The following example shows how to enable time-stamping on logging messages using the current time and date in Coordinated Universal Time/Greenwich Mean Time (UTC/GMT), and enable the year to be displayed:

```
Device(config)# service timestamps log datetime show-timezone year
 Device(config)# end
! The following line shows the timestamp with datetime (11:13 PM March 22nd)
.Mar 22 2004 23:13:25 UTC: %SYS-5-CONFIG_I: Configured from console by console
```

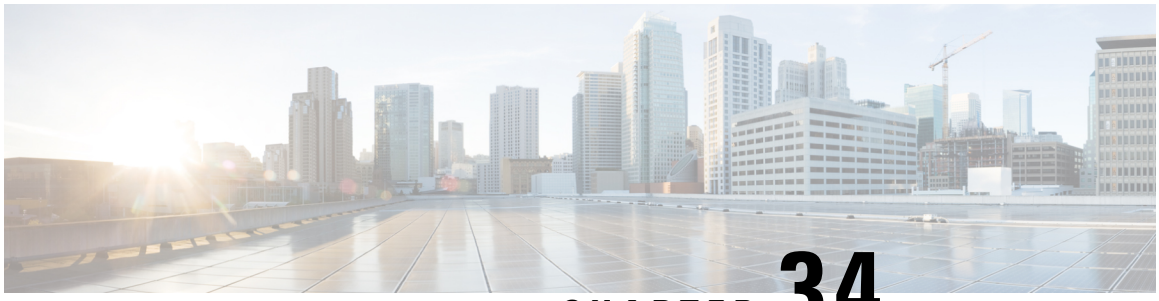
In the following example, the **service timestamps log datetime** command is used to change previously configured options for the date-time time stamp.

```
Device(config)# service timestamps log datetime localtime show-timezone
Device(config)# end
! The year is not displayed.
Oct 13 15:44:46 PDT: %SYS-5-CONFIG_I: Configured from console by console

Enter configuration commands, one per line.  End with the end command.
Device(config)# service timestamps log datetime show-timezone year
Device(config)# end

! note: because the localtime option was not specified again, that option is removed from
the output,
and time is displayed in UTC (the default)

Oct 13 2004 22:45:31 UTC: %SYS-5-CONFIG_I: Configured from console by console
```



CHAPTER 34

MACsec Commands

- key chain, on page 455
- key, on page 456
- **key-string**, on page 457
- cryptographic-algorithm, on page 458
- lifetime, on page 459
- mka policy, on page 460
- confidentiality-offset, on page 461
- delay-protection, on page 461
- include-icv-indicator, on page 462
- key-server, on page 462
- macsec-cipher-suite, on page 463
- sak-rekey, on page 463
- use-updated-eth-header, on page 464
- mka pre-shared-key, on page 465
- fallback-key, on page 465
- macsec access-control, on page 466
- replay-protection window-size, on page 467
- eapol, on page 468
- eapol destination-address, on page 468

key chain

To create or modify a key chain, use the **key chain** command in the key chain configuration mode. To remove this configuration, use the **no** form of this command.

key chain *key-chain-name* **macsec**
no key chain *key-chain-name* **macsec**

Syntax Description

key-chain-name	Specifies the name of the keychain. The maximum length is 32 (128-bit encryption)/64 (256-bit encryption) character hexadecimal string.
macsec	Specifies the key chain for MACsec encryption.

Command Default No default behavior or values.

Command Modes Key chain configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	Command qualified for use in Cisco vManage templates.

Examples The following example shows how you can configure a key chain for MACsec encryption:

```
Device(config)# key chain mac_chain macsec
Device(config-mac_chain-MacSec)#
```

key

To create or modify a keychain key, use the **key** command in keychain-key configuration mode. To remove this configuration, use the **no** form of this command.

key *key-id*
no key *key-id*

Syntax Description

key-id	Hexadecimal string of 2 - 64 characters.

Command Default No default behavior or values.

Command Modes Key chain configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	Command qualified for use in Cisco vManage templates.

Usage Guidelines The key must be of even number of hex characters. Entering an odd number of characters will exit the MACsec configuration mode.

Examples The following example shows how to use the **key** command:

```
Device(config)# key chain mac_chain macsec
Device(config-mac_chain-MacSec)# key 1234abcd5678
```

key-string

To specify the text string for the key, use the **key-string** command in key configuration submode under the macsec key chain mode.

To remove this configuration, use the **no** form of this command.

key-string [**clear** | **password** | **password6**] *key-string-text* **cryptographic-algorithm** { **aes-128-cmac** | **aes-256-cmac** }
no key-string [**clear** | **password** | **password6**] *key-string-text* **cryptographic-algorithm** { **aes-128-cmac** | **aes-256-cmac** }

Syntax Description

clear	Specifies the key string in clear-text form.
password	Specifies the key in encrypted form.
password6	Specifies the key in Type 6 encrypted form.
key-string-text	Text string for the key, which is encrypted by the parser process before being saved to the configuration. The text string has the following character limitations: • Plain-text key strings—Minimum of 1 character and a maximum of 32 (128-bit encryption)/64 (256-bit encryption) characters (hexadecimal string). • Encrypted key strings—Minimum of 4 characters and no maximum.

Command Default

The default value is clear.

Command Modes

Key configuration submode under the macsec key chain mode.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	Command qualified for use in Cisco vManage templates.

Usage Guidelines

For an encrypted password to be valid, the following statements must be true:

- String must contain an even number of characters, with a minimum of four.
- The first two characters in the password string must be decimal numbers and the rest must be hexadecimals.
- The first two digits must not be a number greater than 53.

Either of the following examples would be valid encrypted passwords:

1234abcd or 50aefd

Examples

The following example shows how to use the **key-string** command:

For AES 128-bit encryption:

```
Device(config)# key chain mac_chain macsec
Device(config-mac_chain-MacSec)# key 1234abcd5678
Device(config-mac_chain-MacSec-1234abcd5678)# key-string 12345678123456781234567812345678
cryptographic-algorithm AES-128-CMAC
```

For AES 256-bit encryption with clear-text CAK:

```
Device(config)# key chain mac_chain macsec
Device(config-mac_chain-MacSec)# key 1234abcd5678
Device(config-mac_chain-MacSec-1234abcd5678)# key-string clear
12345678123456781234567812345678123456781234567812345678123456781234567812345678 cryptographic-algorithm
AES-256-CMACRP/0/RP0/CPU0:router(config-mac_chain-MacSec-1234abcd5678)#commit
```

cryptographic-algorithm

Configures the cryptographic algorithm used for authenticating a peer for MACsec encryption in the Keychain-key configuration mode.

To disable this feature, use the **no** form of this command.

cryptographic-algorithm *authentication algorithm*
no cryptographic-algorithm *authentication algorithm*

Syntax Description

authentication algorithm	Configures the 128-bit or 256-bit AES encryption algorithm.

Command Default

No default behavior or values.

Command Modes

Keychain-key configuration.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	Command qualified for use in Cisco vManage templates.

Usage Guidelines

If you do not specify the cryptographic algorithm, MAC computation and API verification would be invalid.

Examples

The following example shows how to use the cryptographic-algorithm command for MACsec Encryption:

```
Device(config-mac_chain-MacSec)# key 1234abcd5678
Device(config-mac_chain-MacSec-1234abcd5678)# key-string 11111111111111111111111111111111
cryptographic-algorithm aes-256-cmac
```

```
Examples

The following example shows how to use the AES-128-CMAC authentication algorithm command:
```

```
Device# key chain mac_chain macsec
Device(config-mac_chain-MacSec)# key 1234abcd5678
Device(config-mac_chain-MacSec-1234abcd5678)# key-string 12345678123456781234567812345678
cryptographic-algorithm aes-128-cmac


Examples

The following example shows how to use the AES-256-CMAC authentication algorithm command:

Device# key chain mac_chain macsec
Device(config-mac_chain-MacSec) # key 1234abcd5678
Device(config-mac_chain-MacSec-1234abcd5678)# key-string 1234567812345678123456781234567812
```

lifetime

Configures the validity period for the MACsec key or CKN in the Keychain-key configuration mode. To disable this feature, use the **no** form of this command.

The lifetime period can be configured with a duration in seconds, as a validity period between two dates (for example, Jan 01 2014 to Dec 31 2014), or with an infinite validity.

The key is valid from the time you configure in HH:MM:SS format. Duration is configured in seconds.

When a key has expired, the MACsec session is torn down and running the show macsec mka session command does not display any information. If you run the show macsec mka interface and show macsec mka interface detail commands, you can see that the session is unsecured.

cryptographic-algorithm *start_time start_date* { *end_time end_date* | **duration** *validity* | **infinite** }
no cryptographic-algorithm *start_time start_date* { *end_time end_date* | **duration** *validity* | **infinite** }

Syntax Description

start_time	Start time in hh:mm:ss from which the key becomes valid. The range is from 0:0:0 to 23:59:59.
end_time	End time in hh:mm:ss at which point the key becomes invalid. The range is from 0:0:0 to 23:59:59.
start_date	The date in DD month YYYY format that the key becomes valid.
end_date	The date in DD month YYYY format that the key becomes invalid.
duration*validity*	The key chain is valid for the duration you configure. You can configure duration in seconds.
infinite	The key chain is valid indefinitely.

Command Default

No default behavior or values.

Command Modes

Keychain-key configuration.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	Command qualified for use in Cisco vManage templates.

Examples

The following example shows how to use the lifetime command:

```
! For AES 128-bit encryption

Device(config)# key chain mac_chain macsec
Device(config-mac_chain-MacSec)# key 1234abcd5678
Device(config-mac_chain-MacSec-1234abcd5678)# key-string 12345678123456781234567812345678
cryptographic-algorithm AES-128-CMAC
Device(config-mac_chain-MacSec-1234abcd5678)# lifetime 05:00:00 20 february 2015 12:00:00
30 september 2016

! For AES 256-bit encryption

Device(config)# key chain mac_chain macsec
Device(config-mac_chain-MacSec)# key 1234abcd5678
Device(config-mac_chain-MacSec-1234abcd5678)# key-string
1234567812345678123456781234567812345678123456781234567812345678 cryptographic-algorithm
AES-256-CMAC
Device(config-mac_chain-MacSec-1234abcd5678)# lifetime 05:00:00 20 february 2015 12:00:00
30 september 2016
```

mka policy

To configure an MKA policy, use the **mka policy** command in Global Configuration mode. To disable this feature, use the **no** form of this command.

mka policy *policy-name*
no mka policy *policy-name*

Syntax Description

policy-name	Name of the MACsec policy for encryption.

Command Default

No default behavior or values.

Command Modes

Global Configuration mode

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	Command qualified for use in Cisco vManage templates.

Examples

The following example shows how to use the **macsec-policy** command:

```
Device(config)# mka policy MKAPolicy
```

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

Command Default Confidentiality offset is disabled.

Command Modes MKA-policy configuration (config-mka-policy)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	Command qualified for use in Cisco vManage templates.

Examples The following example shows how to enable the **confidentiality offset** command:

```
Device(config)# mka policy mka-policy
Device(config-mka-policy)# confidentiality-offset
```

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

Command Default Delay protection for sending MKPDUs is disabled.

Command Modes MKA-policy configuration (config-mka-policy)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	Command qualified for use in Cisco vManage templates.

Examples The following example shows how to configure MKA to use delay protection in sending MKPDUs:

```
Device(config-mka-policy)# delay-protection
```

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

Command Default ICV indicator is included.

Command Modes MKA-policy configuration (config-mka-policy)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	Command qualified for use in Cisco vManage templates.

Examples The following example shows how to include the ICV indicator in MKPDU:

```
Device(config)# mka policy 2
Device(config-mka-policy)# include-icv-indicator
```

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 *value*

Syntax Description

priority*value*	Specifies the priority value of the MKA key-server.

Command Default MKA key-server is disabled.

Command Modes MKA-policy configuration (config-mka-policy)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	Command qualified for use in Cisco vManage templates.

Examples The following example shows how to configure the MKA key-server:

```
Device(config)# mka policy 2
Device(config-mka-policy)# key-server priority 33
```

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** | **gcm-aes-xpn-128** | **gcm-aes-xpn-256** }

no macsec-cipher-suite { **gcm-aes-128** | **gcm-aes-256** | **gcm-aes-xpn-128** | **gcm-aes-xpn-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.
gcm-aes-xpn-128	Configures cipher suite for deriving SAK with 128-bit encryption for Extended Packet Numbering (XPN).
gcm-aes-xpn-256	Configures cipher suite for deriving SAK with 256-bit encryption for XPN.

Command Default

GCM-AES-128 encryption is enabled.

Command Modes

MKA-policy configuration (config-mka-policy)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	Command qualified for use in Cisco vManage templates.

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(config)# mka policy 2
Device(config-mka-policy)# macsec-cipher-suite gcm-aes-256
```

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** *time-interval* | **on-live-peer-loss** }

Syntax Description

interval*time-interval*	SAK rekey interval in seconds. The range is from 30 to 65535, and the default is 0.
on-live-peer-loss	Peer loss from the live membership.

Command Default

The SAK rekey timer is disabled. The default is 0.

Command Modes

MKA-policy configuration (config-mka-policy)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	Command qualified for use in Cisco vManage templates.

Examples

The following example shows how to configure the SAK rekey interval:

```
Device(config)# mka policy 2
Device(config-mka-policy)# sak-rekey interval 300
```

use-updated-eth-header

To enable interoperability between devices and any port on a device that includes the updated Ethernet header in MACsec Key Agreement Protocol Data Units (MKPDUs) for integrity check value (ICV) calculation, use the **ssci-based-on-sci** command in MKA-policy configuration mode. To disable the updated ethernet header in MKPDUs for ICV calculation, use the **no** form of this command.

use-updated-eth-header
no use-updated-eth-header

Command Default

The Ethernet header for ICV calculation is disabled.

Command Modes

MKA-policy configuration (config-mka-policy)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	Command qualified for use in Cisco vManage templates.

Usage Guidelines

The updated Ethernet header is non-standard. Enabling this option ensures that an MACsec Key Agreement (MKA) session between the devices can be set up.

Examples

The following example shows how to use the **key** command:

```
Device(config)# mka policy 2
Device(config-mka-policy)# use-updated-eth-header
```

mka pre-shared-key

To configure MACsec Key Agreement (MKA) MACsec on a device interface using a Pre Shared Key (PSK), use the **mka pre-shared-key key-chain** command in interface configuration mode. To disable it, use the **no** form of this command.

mka pre-shared-key key-chain *key-chain-name*
no mka pre-shared-key key-chain *key-chain-name*

Syntax Description

mka pre-shared-key key-chain	Enables MACsec MKA configuration on device interfaces using a PSK.

Command Default

MKA pre-shared-key is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	Command qualified for use in Cisco vManage templates.

Examples

This example shows how to configure MKA MACsec on an interface using a PSK:

```
Device(config)# interface Gigabitethernet 1/0/20
Device(config-if)# mka pre-shared-key key-chain kc1
```

fallback-key

To provide an alternative fallback option to maintain secure communications, use the **fallback-key** command in Interface configuration mode. Use the **fallback-key** command along with the **mka pre-shared-key key-chain** command. The **mka pre-shared-key key-chain** command is used to enable MKA with a pre-shared key for MACsec encryption on a specified interface.

To remove this configuration, use the **no** form of this command.

mka pre-shared-key key-chain *keychain-name* [**fallback-key-chain** *fallback-keychain-name*]
no mka pre-shared-key key-chain *keychain-name* **fallback-key-chain** *fallback-keychain-name*

Syntax Description

keychain-name	Used as the primary key chain for MKA.
fallback-keychain-name	Used as the fallback key chain for MKA.

Command Default No default behavior or values.

Command Modes Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	Command qualified for use in Cisco vManage templates.

Usage Guidelines The provided configuration enables MKA with a pre-shared key for MACsec encryption on the specified interface (TenGigabitEthernet 0/0/5).

MKA provides secure key agreement for MACsec, which is used to encrypt traffic on the interface.

The primary key-chain is used to store the primary pre-shared key .

MACsec's fallback key feature establishes an MKA session with the pre-shared fallback key whenever the pre-shared key fails to establish a session because of key mismatch.

Fallback key chain supports infinite lifetime with one key only. The connectivity association key name (CKN) ID used in the fallback key chain must not match any of the CKN IDs used in the primary key chain.

Examples The following example shows how to use the **fallback-key** command:

```
Device(config-keychain)# interface TenGigabitEthernet 0/0/5
Devcie(config-if)# mka pre-shared-key key-chain mka-keychain128 fallback-key-chain
mka-keychain256
```

macsec access-control

To control the behavior of unencrypted packets, use the **macsec access-control** command in Interface configuration mode. To disable this option, use the **no** form of this command.

macsec access-control { **must-secure** | **should-secure** }
no macsec access-control { **must-secure** | **should-secure** }

Syntax Description

must-secure	Allows unencrypted packets from the physical interface or subinterfaces to be transmitted or received.
should-secure	Allow unencrypted packets from physical interface or subinterfaces to be transmitted or received. All such packets are dropped except for MKA control protocol packets.

Command Default No default behavior or values.

Command Modes Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	Command qualified for use in Cisco vManage templates.

Usage Guidelines

The **macsec access-control** command can only be configured on physical interface, and the setting is automatically inherited by the subinterfaces.

Examples

The following example shows how to use the **macsec access-control** command:

```
Device(config)#interface GigabitEthernet0/0/1
Device(config-if)# macsec access-control must-secure

Device(config)#interface GigabitEthernet0/0/1
Device(config-if)# macsec access-control should-secure
```

replay-protection window-size

To change the replay window size, use the **replay-protection window-size** command in Interface configuration mode. The range for window size is 0 to 4294967295. To turns off MACsec replay-protection, use the **no** form of this command.

replay-protection window-size *frames*
no replay-protection window-size

Syntax Description

frames	Enable replay protection, and configure the window size in number of frames. The range is from 0 to 4294967295. The default window size is 0.

Command Default

No default behavior or values.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	Command qualified for use in Cisco vManage templates.

Usage Guidelines

Replay protection is a feature provided by MACsec to counter replay attacks. Each encrypted packet is assigned a unique sequence number and the sequence is verified at the remote end. Frames transmitted through a Metro Ethernet service provider network are highly susceptible to reordering due to prioritization and load balancing mechanisms used within the network.

A replay window is necessary to support use of MACsec over provider networks that reorder frames. Frames within the window can be received out of order, but are not replay protected. The default window size is set to 64.

The replay protection window may be set to zero to enforce strict reception ordering and replay protection.

Note A replay protection window can be configured independently on either physical interface or subinterface. If it is configured on the physical interface, it is automatically inherited by the subinterfaces. Explicit configuration on subinterface overrides the inherited value or policy for that sub-interface.

Examples

The following example shows how to use the **replay-protection window-size** command:

```
Device(config)#interface GigabitEthernet0/0/1
Device(config-if)# macsec replay-protection window-size 10
```

eapol

To configures an ethernet type (Hexadecimal) for the EAPoL Frame on the interface, use the **eapol** command in Interface configuration mode. To disble this option, use the **no** form of this command.

eapol *eth-type*
no eapol *eth-type*

Syntax Description

eth-type	Configures an ethernet type (Hexadecimal) for the EAPoL Frame on the interface.

Command Default No default behavior or values.

Command Modes Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	Command qualified for use in Cisco vManage templates.

Examples

The following example shows how to use the **eapol***eth-type* command:

```
Device(config)#interface GigabitEthernet0/0/1
Device(config-if)# eapol eth-type 0xB860
```

eapol destination-address

To change the destination MAC address of an EAPoL packet that is transmitted on an interface towards the service provider, use the **eapol destination-address** command in Interface configuration mode. To disable this option,, use the **no** form of this command.

eapol destination-address [*MAC-Address* | { **bridge-group-address** | **broadcast-address** | **lldp-multicast-address** }]

no eapol destination-address [*MAC-Address* | { **bridge-group-address** | **broadcast-address** | **lldp-multicast-address** }]

Syntax Description

MAC-Address	Configures an Extensible Authentication Protocol over LAN (EAPoL) destination MAC address on the interface.
bridge-group-address	Sets the destination address as a bridge group.
broadcast-address	Sets the destination address as a broadcast address.
lldp-multicast-address	Sets the destination address as a LLDP multicast address.

Command Default

No default behavior or values.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	Command qualified for use in Cisco vManage templates.

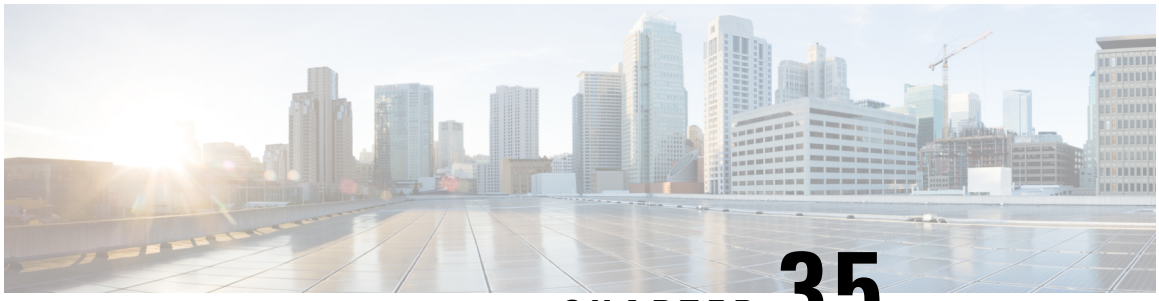
Usage Guidelines

When the eapol destination-address command is configured on the main interface, it is applied to any subinterfaces on that interface. However, if the eapol destination-address command is configured on the subinterface, that takes take precedence over the command on the main interface.

Examples

The following example shows how to use the **eapol destination-address** command:

```
Device(config)#interface GigabitEthernet0/0/1
Device(config-if)# eapol destination-address 0018.b967.3cd0
Device(config-if)# eapol destination-address bridge-group-address
Device(config-if)# eapol destination-address broadcast-address
Device(config-if)# eapol destination-address lldp-multicast-address
```



CHAPTER 35

Multi-Region Fabric

- affinity-group (Multi-Region Fabric), on page 471
- affinity-group-number, on page 472
- affinity-group preference (Multi-Region Fabric), on page 473
- filter route outbound affinity-group preference (Multi-Region Fabric), on page 473
- management-gateway, on page 474
- management-region, on page 475
- omp best-path region-path-length ignore (Multi-Region Fabric), on page 477
- omp best-path transport-gateway, on page 477
- region (Multi-Region Fabric), on page 478
- region access, region core (Multi-Region Fabric), on page 479
- role (Multi-Region Fabric), on page 480
- transport-gateway (Multi-Region Fabric), on page 481

affinity-group (Multi-Region Fabric)

Use the **affinity-group** command in system configuration mode to configure an affinity group for an edge router or border router. Use the **no** form of the command to remove the affinity group assignment.

affinity-group *group-id*

no affinity-group

Syntax Description

group-id	Affinity group in the range 1 to 63.

Command Default

By default, no affinity group is assigned.

Command Modes

System configuration (config-system)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	This command was introduced.

Usage Guidelines If an affinity group has been configured previously on the device, configuring a new value replaces the previous.

Example

Configure an affinity group value of 10 on a border router.

```
Device#config-transaction
Device(config)#system
Device(config-system)#affinity-group 10
```

affinity-group-number

To assign an affinity group number to routes or TLOCs, in a Multi-Region Fabric environment, use the **affinity-group-number** command in configuration set mode when configuring a control policy on a Cisco SD-WAN Controller. To cancel the configuration, use the **no** form of the command.

affinity-group-number *affinity-group*
no affinity-group-number *affinity-group*

Syntax Description

affinity-group-number *affinity-group*	Assign an affinity group number in the range of 0 to 63.

Command Default There is no default.

Command Modes configuration set (config-set)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	This command was introduced.

Example

The following example, executed on a Cisco SD-WAN Controller, creates a sequence that matches routes from devices at site 100 and assigns them the affinity group 5.

```
vsmart# config
vsmart(config)# policy
vsmart(config-policy)# control-policy policy-1
vsmart(config-control-policy-cpolicy1)# sequence 1
vsmart(config-sequence-1)# match route
vsmart(config-match-route)# site-id 100
vsmart(config-match-route)# action accept
vsmart(config-action)# set
vsmart(config-set)# affinity-group-number 5
```

To configure this using a CLI template in Cisco SD-WAN Manager, use the following:

```
policy
 control-policy policy-1
  sequence 1
   match route
    site-id 100
```

```
  !
  action accept
   set
    affinity-group-number 5
   !
  !
 !
!
```

affinity-group preference (Multi-Region Fabric)

Use the **affinity-group preference** command in system configuration mode to configure the affinity group preference order, from highest priority to lowest priority. Use the **no** form of the command to remove the affinity group preference.

affinity-group preference *group-id*
group-id **. . .**

no affinity-group preference

Syntax Description

group-id	Affinity group in the range 1 to 63.

Command Default

By default, no affinity group preference is assigned.

Command Modes

System configuration (config-system)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	This command was introduced.

Example

Configure a preference for affinity groups 10, 11, 20, and 5, in that order of priority.

```
Device#config-transaction
Device(config)#system
Device(config-system)#affinity-group preference 10 11 20 5
```

filter route outbound affinity-group preference (Multi-Region Fabric)

To configure a Cisco SD-WAN Controller to restrict routers in the regions that it is managing to connect only to routers that are on their affinity list, use the **filter route outbound affinity-group preference** command in OMP configuration mode. To remove this restriction, use the **no** form of the command.

filter route outbound affinity-group preference

no filter route outbound affinity-group preference

Command Default By default, there is no restriction.

Command Modes OMP configuration (config-omp)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	This command was introduced.

Usage Guidelines You can configure Cisco Catalyst SD-WAN to enable routers to connect only to routers that are on their affinity list. To do this, use the **filter route outbound affinity-group preference** command on each of the Cisco SD-WAN Controllers that manage a region.

Example

```
vSmart#config terminal
vSmart(config)#omp
vSmart(config-omp)#filter route outbound affinity-group preference
```

management-gateway

To enable a management region on a router configured as a management gateway, use the **management-gateway** command in system configuration mode. Use the **no** form of the command to disable a management region.

management-gateway enable

no management-gateway enable

Command Default Management region is disabled

Command Modes System configuration (config-system)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.13.1a	This command was introduced.

Example 1

The following sample configuration configures a management gateway to support a management region, using VRF 3:

```
Device(config)# system
Device(config-system)# region 1
Device(config-region-1)# management-region
Device(config-management-region)# vrf 3
```

```
Device(config-vrf-3)# exit
Device(config-system)# management-gateway enable
```

Related Commands

Command	Description
management-region	Use the **management-region** command to enable a management region on a Cisco SD-WAN Controller or on a router.

management-region

To enable a management region on a Cisco SD-WAN Controller or on a router, use the **management-region** command in system configuration mode or region configuration mode, respectively. Use the **no** form of the command to disable a management region.

For a Cisco SD-WAN Controller:

management-region

no management-region

For a router:

management-region vrf *vrf-id* [**gateway-preference** *preference-id* [*preference-id*] **. . .**]

no management-region

Syntax Description

vrf *vrf-id*	Configure the VRF to use for management traffic.
gateway-preference *preference-id*	Configure a preference order among management gateways, according to the affinity group number of the management gateways. See the Usage Guidelines section. Maximum number of affinity group numbers: 12

Command Default

Management region is disabled

Command Modes

System configuration (config-system)
Region configuration (config-region)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.13.1a	This command was introduced.

Usage Guidelines

We recommend dedicating one or more Cisco SD-WAN Controllers to exclusively manage the management region. Alternatively, you can use one or more Cisco SD-WAN Controllers that are managing the core region. A Cisco SD-WAN Controller that is managing an access region cannot also manage the management region.

Configuring an affinity group number is optional, but when you are configuring a router in the network, you can configure a preference order among multiple management gateways, according to their affinity group numbers.

On management gateways, you can use the following to configure affinity group numbers:

- System-level affinity group for the router:

  Use the **affinity-group affinity-group-number** *affinity-group* command.

- Per-VRF affinity group:

  Use the **affinity-group affinity-per-vrf** *affinity-group* **vrf-range** *vrf-range* command.

  The per-VRF affinity group takes precedence over the system-level affinity group.

For information, see affinity-group-number.

Example 1

The following configures a Cisco SD-WAN Controller that is managing region 0, to also support a management region.

```
Controller(config)# system
Controller(config-system)# region 0
Controller(config-system)# management-region
```

Example 2

The following sample configuration configures a management gateway to support a management region, using VRF 3. Configuring the affinity group number is optional, but when you are configuring a router in the network, you can configure a preference order among multiple management gateways, according to affinity group number.

```
Device(config)# system
Device(config-system)# region 1
Device(config-region-1)# management-region
Device(config-management-region)# vrf 3
Device(config-vrf-3)# exit
Device(config-system)# management-gateway enable
Device(config-system)# affinity affinity-group-number 1
```

Example 3

The following sample configuration configures a border router to support a management region using VRF 3, and configures a gateway preference order:

```
Device(config)# system
Device(config-system)# system-ip 10.1.1.2
Device(config-system)# domain-id 1
Device(config-system)# site-id 100
Device(config-system)# region 1
Device(config-region-1)# management-region vrf 3 gateway-preference 1 2
Device(config-vrf-3)# exit
Device(config-management-region)# exit
Device(config-region-1)# exit
Device(config-system)# role border-router
```

Related Commands

Command	Description
management-gateway	Use the **management-gateway** command to enable a management region on a router functioning as a management gateway.

omp best-path region-path-length ignore (Multi-Region Fabric)

To configure a device operating with Cisco Catalyst SD-WAN to enable both the primary region path and the secondary region path to a peer device, use the **omp best-path region-path-length ignore** command in global configuration mode. To return to the default behavior, use the **no** form of the command.

omp best-path region-path-length ignore

no omp best-path region-path-length ignore

Command Default

By default, the overlay management protocol (OMP) considers the path length when determining the best paths to provide to the forwarding layer.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	Added the following options for configuring secondary regions: **secondary-region**, **secondary-shared**, **secondary-only**

Usage Guidelines

When a direct path is available to reach a destination, by default the overlay management protocol (OMP) provides only the direct path to the routing forwarding layer because the direct path uses fewer hops. The result is that the forwarding layer, which includes application-aware policy, can only use the direct path. You can use this command to disable this comparison of the number of hops so that traffic can use either the direct secondary-region path (fewer hops) or the primary-region path (more hops). When you disable the comparison of the number of hops, OMP applies equal-cost multi-path routing (ECMP) to all routes, and packets can use all available paths.

Examples

```
Device(config)#omp best-path region-path-length ignore
```

omp best-path transport-gateway

Use the **omp best-path transport-gateway** command in OMP configuration mode to configure the path preference for transport gateway paths. Use the **no** form of the command to restore the default behavior.

omp best-path transport-gateway { **ecmp-with-direct-path** | **prefer** } [**transport-gateway-settings** *site-types-list*]

no omp best-path transport-gateway

Syntax Description

ecmp-with-direct-path	For devices that can connect through a transport gateway and through other paths, apply equal-cost multi-path (ECMP) logic to choose the best path. This is the default behavior.
prefer	For devices that can connect through a transport gateway, use only the transport gateway paths, even if other paths are available.
transport-gateway-settings *site-types-list*	When configuring a router to prefer a transport gateway path, restrict the preference to only traffic whose destination matches one or more specific site types. For information about configuring a site type for a router, and for a list of site types, see **site-type**.

Command Default

ecmp-with-direct-path

Command Modes

OMP configuration (config-omp)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	This command was introduced.
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	Added **transport-gateway-settings** *site-type*, which enables you to specify which traffic will prefer a transport gateway route.

The following example configures a device to prefer transport gateway routes.

```
Device(config)#omp best-path transport-gateway prefer
```

The following example configures a device to prefer transport gateway routes only for traffic destined to sites with site type cloud.

```
Device(config)#omp best-path transport-gateway prefer
Device(config)#omp best-path transport-gateway-settings site-types cloud
```

Related Commands

Command	Description
site-type	Use the **site-type** command to configure the site type of a router.

region (Multi-Region Fabric)

To assign a region to a device, use the **region** command in system configuration mode. Use the **no** form of the command to remove the region assignment.

region *region-id*
subregion *subregion-id*

no region

Syntax Description

region *region-id*	Assign a region in the range of 1 to 63.
subregion *subregion-id*	Assign a subregion in the range of 1 to 63.

Command Default

The command has no default.

Command Modes

System configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.x	This command was introduced.
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	Added the **subregion** option.

Usage Guidelines

Example

The following example configures a device to region 1, subregion 5.

```
system
 system-ip 192.0.2.1
 domain-id 1
 site-id 1100
 region 1
  subregion 5
```

region access, region core (Multi-Region Fabric)

To configure a border router in a Multi-Region Fabric environment that is performing route aggregation to advertise the routes specifically to the core region or access region, use the **region access** or **region core** commands in VRF configuration mode. To cancel the configuration, use the **no** form of the command. For a border router performing route aggregation, we recommend configuring either **region core** or **region access**.

advertise aggregate *prefix*
aggregate-only
region { **access** | **core** }

no advertise aggregate *prefix* [**aggregate-only**]
region { **access** | **core** }

Syntax Description

aggregate-only	Use **aggregate-only** to advertise only the aggregate prefix and not the component routes included within the range of the prefix.
region {**access** | **core**}	When using route aggregation on a border router, advertise aggregated routes to the access region or to the core region. If you do not specify the region, the border router advertises the aggregated routes both to the access region that it serves and to the core region.

Command Default The command has no default.

Command Modes VRF configuration (config-vrf-vrf-number)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	This command was introduced.

Example

The following example, executed on a border router in a Multi-Region Fabric environment, advertises aggregation of routes defined by the 10.0.0.0/8 prefix. The border router advertises the routes to its peers in the core region. This is useful for aggregating routes for access region devices in the 10.0.0.0/8 range to reduce the number of routes that must be advertised in the core region.

```
Device#config-transaction
admin connected from 127.0.0.1 using console on vm11
Device(config)#sdwan omp
Device(config-omp)#address-family ipv4 vrf 1
Device(config-vrf-1)#advertise aggregate 10.0.0.0/8 region core
```

The following example, executed on a border router in a Multi-Region Fabric environment, advertises aggregation of routes defined by the 10.0.0.0/8 prefix. The border router advertises the routes to its peers in the access region. This is useful for aggregating routes for core region devices in the 10.0.0.0/8 range to reduce the number of routes that must be advertised in the access region.

```
Device#config-transaction
admin connected from 127.0.0.1 using console on vm11
Device(config)#sdwan omp
Device(config-omp)#address-family ipv4 vrf 1
Device(config-vrf-1)#advertise aggregate 10.0.0.0/8 region access
```

role (Multi-Region Fabric)

To configure a device role as border router for Multi-Region Fabric, use the **role** command in system configuration mode. To configure a device to the default edge router mode, use the **no** form of this command.

role border-router

no role

Syntax Description

border-router	Configure the device role as border router.

Command Modes System configuration (config-system)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

The command does not have an option for setting the role to edge router. The default role is edge router, so you can use the **no** form of the command to configure the device role as edge router.

Examples

Configure a device role as border router.

```
Device(config)#system
Device(config-system)#role border-router
```

Examples

Configure a device role as edge router.

```
Device(config)#system
Device(config-system)#no role
```

transport-gateway (Multi-Region Fabric)

Use the **transport-gateway** command in system configuration mode to enable transport gateway functionality on a device. Use the **no** form of the command to disable this functionality.

transport-gateway enable

no transport-gateway enable

Command Default

By default, transport gateway functionality is disabled.

Command Modes

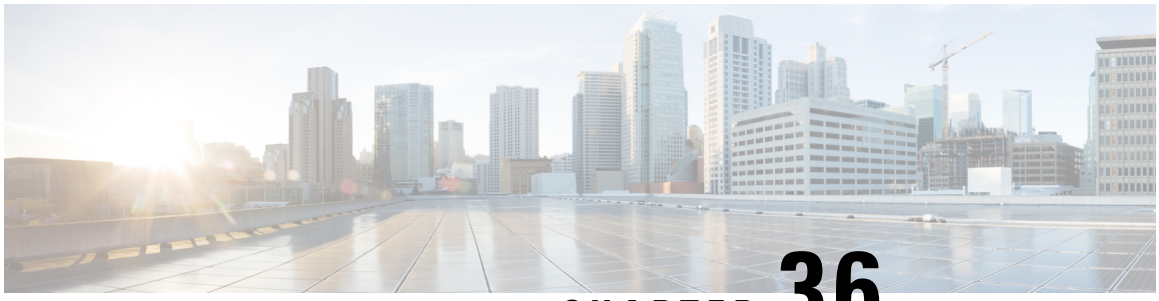
System configuration mode (config-system)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	This command was introduced.

Example

```
Device(config-system)#transport-gateway enable
```



CHAPTER 36

NAT Commands

- ip nat, on page 483
- ip nat inside source, on page 484
- ip nat inside source tcp static interface (loopback), on page 488
- ip nat log translations flow-export, on page 489
- ip nat outside source, on page 490
- ip nat pool, on page 492
- ip nat route vrf, on page 493
- ip nat service, on page 494
- ip nat settings preserve-sdwan-ports, on page 495
- ip nat translation (timeout), on page 496
- ip nat translation max-entries, on page 497
- nat64 provisioning, on page 498
- nat64 route, on page 500
- nat64 settings, on page 501
- nat64 settings mtu, on page 502
- nat64 translation timeout tcp, on page 503
- nat64 translation timeout udp, on page 503
- nat66 max vpn, on page 504
- nat66 outside, on page 505
- nat66 prefix, on page 505
- nat66 route vrf, on page 507

ip nat

To designate that traffic originating from the interface is subject to Network Address Translation (NAT), use the **ip nat** command in interface configuration mode. To designate that traffic originating from the interface is no longer subject to Network Address Translation (NAT), use the **no** form of this command.

ip nat outside
no ip nat outside

Syntax Description

outside	(Optional) Indicates that the interface is connected to the outside network.

Command Default Traffic leaving or arriving at this interface is not subject to NAT.

Command Modes Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Qualified for use in Cisco vManage CLI templates

Usage Guidelines For the usage guidelines, see ip nat.

Examples

```
Device(config)# interface Ethernet 1
 Device(config-if)# ip nat outside
```

ip nat inside source

To enable Network Address Translation (NAT) of the inside source address, use the **ip nat inside source** command in global configuration mode. To remove the static translation, or the dynamic association to a pool, use the **no** form of this command.

Dynamic NAT
ip nat inside source list { *access-list-number access-list-name* } **pool** *name* [**vrf** *name*] [**match-in-vrf** | **overload**] [**match-interface** | { *interface-name* }]
no ip nat inside source list { *access-list-number access-list-name* } **pool** *name* [**vrf** *name*] [**match-in-vrf** | **overload**] [**match-interface** | { *interface-name* }]

Static NAT
ip nat inside source static *local-ip global-ip* [**vrf** *name*] [**match-in-vrf** [**track** *track-id*] [**pool** *name*] | **pool** *name* | **no-payload** { **match-in-vrf** [**pool** *name*] | **pool** *name* } | [**egress-interface** *type*] | [**extendable**] { [**match-in-vrf** [**pool** *name*]] | **pool** *name* | **no-payload** { **match-in-vrf** [**pool** *name*] | **pool** *name* } }]
no ip nat inside source static *local-ip global-ip* [**vrf** *name*] [**match-in-vrf** [**track** *track-id*] [**pool** *name*] | **pool** *name* | **no-payload** { **match-in-vrf** [**pool** *name*] | **pool** *name* } | [**egress-interface** *type*] | [**extendable**] { [**match-in-vrf** [**pool** *name*]] | **pool** *name* | **no-payload** { **match-in-vrf** [**pool** *name*] | **pool** *name* } }]

Syntax Description

list *access-list-number*	Specifies the number of a standard IP access list. Packets with source addresses that pass the access list are dynamically translated using global addresses from the named pool.
list *access-list-name*	Specifies the name of a standard IP access list. Packets with source addresses that pass the access list are dynamically translated using global addresses from the named pool.
interface	Specifies an interface for the global address.
type	Interface type. For more information, use the question mark (?) to enable the online help function.

number	Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) to enable the online help function.
pool *name*	Specifies the name of the pool from which global IP addresses are allocated dynamically. From Cisco IOS XE Catalyst SD-WAN Release 17.5.1a, you can use a NAT pool for static NAT.
overload	(Optional) Enables the device to use one global address for many local addresses. When overloading is configured, the TCP or UDP port number of each inside host distinguishes between the multiple conversations using the same local IP address.
vrf *name*	(Optional) Associates the NAT translation rule with a particular VPN routing and forwarding (VRF) instance.
egress-interface *type*	(Optional) Specifies the type of egress interface used for port forwarding with NAT DIA.
match-in-vrf	(Optional) Enables NAT inside and outside traffic in the same VRF.
match-interface *interface-name*	Specifies the interface name to apply the centralized data policy to for matching a NAT method with a NAT DIA egress interface.
track *track-id*	(Optional) Enables service-side NAT object tracking of LAN prefixes and LAN interfaces.
static	Sets up a single static translation.
local-ip	Local IP address assigned to a host on the inside network. The address could be randomly chosen, allocated from RFC 1918, or be an obsolete one.
global-ip	Globally unique IP address of an inside host as it appears to the outside network.
extendable	(Optional) Extends the translation.
forced	(Optional) Forcefully deletes an entry and its children from the configuration.
tcp	Establishes the TCP protocol.
udp	Establishes the UDP protocol.
local-port	Local TCP or UDP port. The range is from 1 to 65535.
global-port	Global TCP or UDP port. The range is from 1 to 65535.

Command Default No NAT translation of inside source addresses occurs.

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	This command was modified. The **pool** *pool* keyword-argument pair is supported for static NAT.
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	This command was modified. Added the **track** keyword for service-side NAT object tracking.
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This command was modified. Added the **egress-interface** *type* keyword for port forwarding for NAT DIA.
Cisco IOS XE Catalyst SD-WAN Release 17.14.1a	This command was modified. Added the **match-interface** *interface-name* keyword fork mapping multiple NAT methods for NAT DIA.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `ip nat inside source` command.

Examples

The following example shows how to translate between inside hosts addressed from one network to the globally unique network:

```
Device(config)# ip nat pool net-209 10.255.255.254 10.255.255.255 prefix-length 28
ip nat inside source list 1 pool net-209
!
interface ethernet 0
 ip address 10.0.0.1 255.255.255.224
 ip nat outside
!
interface ethernet 1
 ip address 10.255.255.254 10.255.255.255
 ip nat inside
!
access-list 1 permit 192.168.255.255 255.255.0.
access-list 1 permit 192.168.255.255 255.255.224.
```

The following example shows how to translate local traffic to an edge device that is using NAT (NAT-PE):

```
Device(config)# ip nat inside source list 1 interface ethernet 0 vrf vrf1 overload
ip nat inside source list 1 interface ethernet 0 vrf vrf2 overload
!
ip route vrf vrf1 0.0.0.0 0.0.0.0 192.168.255.254
ip route vrf vrf2 0.0.0.0 0.0.0.0 192.168.255.255
!
access-list 1 permit 0.0.0.0 255.0.0.0
!
ip nat inside source list 1 interface ethernet 1 vrf vrf1 overload
ip nat inside source list 1 interface ethernet 1 vrf vrf2 overload
!
ip route vrf vrf1 0.0.0.0 0.0.0.0 192.168.0.0 global
ip route vrf vrf2 0.0.0.0 0.0.0.0 192.168.0.1 global
access-list 1 permit 0.0.0.0 255.0.0.0
```

The following example shows how to configure a NAT pool using static inside NAT.

```
Device(config)# ip nat pool natpool1 10.11.11.1 10.11.11.30 prefix-length 24
ip nat pool natpool2 10.11.11.5 10.11.11.6 prefix-length 24
ip nat inside source list global-list pool natpool1 vrf 1 match-in-vrf
ip nat inside source list global-list pool natpool2 vrf 1 match-in-vrf
ip nat inside source static 192.168.11.10 10.11.11.10 vrf 1 match-in-vrf pool natpool1
```

The following example shows how to configure a NAT pool using static inside and static outside NAT.

```
Device(config)# ip nat pool natpool1 10.11.11.1 10.11.11.30 prefix-length 24
ip nat pool natpool2 10.11.11.5 10.11.11.6 prefix-length 24
ip nat inside source list global-list pool natpool1 vrf 1 match-in-vrf
ip nat inside source list global-list pool natpool2 vrf 1 match-in-vrf
ip nat inside source static 192.168.11.10 10.11.11.10 vrf 1 match-in-vrf pool natpool1
ip nat outside source static 192.168.21.10 10.22.22.10 vrf 1 match-in-vrf pool natpool1
```

The following example shows how to configure an inside static NAT global pool with a tracker name and a tracker ID for tracking service-side NAT objects:

```
Device(config)# ip nat inside source static 192.168.11.10 10.11.11.10 vrf 1 match-in-vrf
track 1
```

For more information on configuring the service-side NAT object tracker, see the *Cisco SD-WAN NAT Configuration Guide*.

The following example shows how to configure NAT DIA port forwarding:

```
Device(config)# interface GigabitEthernet1
ip address 10.1.2.1 255.255.255.0
ip nat outside
negotiation auto
no mop enabled
no mop sysid
end
ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet1 overload
ip nat inside source static tcp 192.168.1.100 443 interface GigabitEthernet1 8443 vrf 1
ip nat inside source static tcp 192.168.1.100 80 10.1.2.10 80 vrf 1 egress-interface
GigabitEthernet1
ip nat inside source static tcp 192.168.1.100 22 10.1.2.20 2020 vrf 1 egress-interface
GigabitEthernet1
```

For more information on configuring NAT DIA port forwarding, see the *Cisco SD-WAN NAT Configuration Guide*.

The following is a sample configuration for configuring multiple NAT DIA where the default NAT method is using a NAT pool and the alternative or secondary NAT method is using interface overload with match-interface:

```
interface GigabitEthernet1
 ip address 10.1.1.1 255.255.255.0
 no ip redirects
 load-interval 30
 negotiation auto
 ip nat outside
 !
 ip nat inside source list dia-list 1 pool natpool1 overload egress-interface GigabitEthernet1

 ip nat inside source list dia-list 1 interface GigabitEthernet1 overload match-interface
GigabitEthernet1
```

For more information about configuring the multiple NAT methods for an interface using CLI, see the section "Configure Multiple NAT Types Using CLI" in Cisco SD-WAN NAT Configuration Guide.

ip nat inside source tcp static interface (loopback)

To enable the loopback interface of the inside source address, use the **ip nat inside source static tcp interface (loopback)** command in global configuration mode.

ip nat inside source static tcp *local-ip local-port* **interface** *interface-type interface-number* [**egress-interface** *interface-type interface-number* | **vrf** *vrf-name* **egress-interface** *interface-type interface-number*]

Syntax Description

local-ip	Local IP address assigned to a host on the inside network.
interface-type interface-number	Specifies the loopback interface type and the loopback interface number.
vrf *name*	(Optional) Associates the NAT translation rule with a particular VPN routing and forwarding (VRF) instance. The VRF keyword along with a VRF name. When you don't specify a value for the VRF number, port forwarding is configured on the transport VPN, which is VPN 0, by default.
egress-interface *interface-type interface-number*	(Optional) Specifies the egress interface type and the egress interface number that are used for port forwarding with NAT DIA with loopback interface.

Command Default

Loopback interface of the inside source address is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	This command is introduced.

Usage Guidelines

Configure the WAN interface before you configure the loopback interface.

Optionally, you can provide the egress interface, for example, **GigabitEthernet1**, which is the internet-facing interface.

The following example shows how to configure port forwarding with NAT DIA by using a loopback interface:

Configure **ip nat outside** on the WAN interface:

```
interface GigabitEthernet1
 ip address 10.1.2.1 255.255.255.0
 ip nat outside
 negotiation auto
 no mop enabled
```

```
 no mop sysid
exit
```

Define the loopback interface:

```
interface Loopback3
 ip address 10.1.3.1 255.255.255.255
exit
```

Configure the loopback interface:

```
ip nat inside source static tcp 192.168.1.100 8080 interface Loopback3 8585 vrf 1
egress-interface GigabitEthernet1
ip nat inside source static tcp 192.168.1.100 80 interface Loopback3 5050 egress-interface
 GigabitEthernet1
```

For more information about configuring the loopback interface, see *Configure Port Forwarding with NAT DIA Using a CLI Template*.

Related Commands

Commands	Description
ip nat	Ensures that traffic originating from the interface is subject to Network Address Translation (NAT)
negotiation [auto]	Specifies enabling the autonegotiation protocol to configure the speed, duplex, and automatic flow control of the Gigabit Ethernet interface.
static	Sets up a single static translation.
tcp	Establishes the TCP protocol.
egress-interface	Specifies the type of egress interface used for port forwarding with NAT DIA using a loopback interface.

ip nat log translations flow-export

To enable the high-speed logging of translations by NAT, use the **ip nat log translations flow-export** command in global configuration mode. To disable the logging of NAT translations by using a flow exporter, use the **no** form of this command.

ip nat log translations flow-export v9 udp { **destination** *IPv4address port* } [**vrf** *vrf-name* | **source** *interface-name interface-number*]
no ip nat log translations flow-export

Syntax Description

v9	Specifies the flow exporter Version 9 format.
udp	Specifies the UDP.
destination	Specifies the destination IPv4 address. It can be IPv4 global (vpn0/transport vpn) or IPv4 vrf (service vpn).
ipv4 address	Specifies the IPv4 address of the destination.

local-udp-port	Specifies the local UDP port number. Valid values are from 1 to 65335.
source *interface-type interface-number*	(Optional) Specifies the source interface for which translations will be logged.
vrf *vrf-name*	(Optional) Specifies the destination VRF.

Command Default

Logging is disabled for all NAT translations.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco IOS XE Release 17.6.4 and later 17.6.x releases	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE ip nat log translations flow-export command.

Examples

The following example shows how to enable translation logging for a specific destination and source interface:

```
Device(config)# ip nat log translations flow-export v9 udp destination 10.10.0.1 1020 source
 gigabithethernet 0/0/1
```

Related Commands

Commands	Description
clear ip nat translations	Clears dynamic NAT translations from the translation table.
show ip nat translations	Displays active NAT translations.

ip nat outside source

To enable Network Address Translation (NAT) of the outside source address, use the **ip nat outside source** command in global configuration mode. To remove the static entry or the dynamic association, use the **no** form of this command.

Dynamic NAT
ip nat outside source { **list** { *access-list-number* *access-list-name* } } **pool** *pool-name* [**vrf** *name*]
no ip nat outside source { **list** { *access-list-number* *access-list-name* } } **pool** *pool-name* [**vrf** *name*]

Static NAT
ip nat outside source static *local-ip global-ip* [**vrf** *name*] [**match-in-vrf** [**pool** *name*] | **pool** *name* | **no-payload** { **match-in-vrf** [**pool** *name*] | **pool** *name* } | [**extendable**] { [**match-in-vrf** [**pool** *name*]] | **pool** *name* | **no-payload** { **match-in-vrf** [**pool** *name*] | **pool** *name* } }]

no ip nat outside source static *local-ip global-ip* [**vrf** *name*] [**match-in-vrf** [**pool** *name*] | **pool** *name* | **no-payload** { **match-in-vrf** [**pool** *name*] | **pool** *name* } | [**extendable**] { [**match-in-vrf** [**pool** *name*]] | **pool** *name* | **no-payload** { **match-in-vrf** [**pool** *name*] | **pool** *name* } }]

Syntax Description

list *access-list-number*	Specifies the number of a standard IP access list. Packets with source addresses that pass the access list are translated using global addresses from the named pool.
list *access-list-name*	Specifies the name of a standard IP access list. Packets with source addresses that pass the access list are translated using global addresses from the named pool.
pool *pool-name*	Specifies the name of the pool from which global IP addresses are allocated. Starting Cisco IOS XE Catalyst SD-WAN Release 17.5.1a, you can use a NAT pool for static NAT.
vrf *name*	(Optional) Associates the NAT rule with a particular VPN routing and forwarding (VRF) instance.
static	Sets up a single static translation.
global-ip	Globally unique IP address assigned to a host on the outside network by its owner. The address was allocated from the globally routable network space.
local-ip	Local IP address of an outside host as it appears to the inside network. The address was allocated from the address space routable on the inside (RFC 1918, *Address Allocation for Private Internets*).
match-in-vrf	(Optional) Matches the incoming VRF.
extendable	(Optional) Extends the transmission.

Command Default

No translation of source addresses coming from the outside to the inside network occurs.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	The **match-in-vrf** keyword is added.
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	This command was modified. The **pool** *pool* keyword-argument pair is supported for Static NAT.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `ip nat outside source` command.

Examples

The following example shows how to translate between inside hosts addressed from the 10.0.0.1 network to the globally unique 10.0.0.0/28 network. Further, packets from outside hosts addressed from the 10.255.255.254 network are translated to appear to be from the 10.255.255.255/24 network.

```
ip nat pool net-208 10.255.255.254 10.255.255.255 prefix-length 28
```

```
ip nat pool net-10 10.255.255.254 10.255.255.255 prefix-length 24
ip nat inside source list 1 pool net-208
ip nat outside source list 1 pool net-10
!
interface ethernet 0
 ip address 10.0.0.1 255.255.255.224
 ip nat outside
!
interface ethernet 1
 ip address 10.0.0.1 255.255.255.224
 ip nat inside
!
access-list 1 permit 10.255.255.254 10.255.255.255
```

Static NAT Inside with NAT Pool

```
ip nat pool natpool1 10.11.11.1 10.11.11.30 prefix-length 24
ip nat pool natpool2 10.11.11.5 10.11.11.6 prefix-length 24
ip nat inside source list global-list pool natpool1 vrf 1 match-in-vrf
ip nat inside source list global-list pool natpool2 vrf 1 match-in-vrf
ip nat inside source static 192.168.11.10 10.11.11.10 vrf 1 match-in-vrf pool natpool1
```

Static NAT Inside and Static NAT Outside with NAT Pool

```
ip nat pool natpool1 10.11.11.1 10.11.11.30 prefix-length 24
ip nat pool natpool2 10.11.11.5 10.11.11.6 prefix-length 24
ip nat inside source list global-list pool natpool1 vrf 1 match-in-vrf
ip nat inside source list global-list pool natpool2 vrf 1 match-in-vrf
ip nat inside source static 192.168.11.10 10.11.11.10 vrf 1 match-in-vrf pool natpool1
ip nat outside source static 192.168.21.10 10.22.22.10 vrf 1 match-in-vrf pool natpool1
```

ip nat pool

To define a pool of IP addresses for Network Address Translation (NAT) translations, use the **ip nat pool** command in global configuration mode. To remove one or more addresses from the pool, use the **no** form of this command.

ip nat pool *name start-ip end-ip* [**prefix-length** *prefix-length*]
no ip nat pool *name*

Syntax Description

name	Name of the pool.
start-ip	Starting IP address that defines the range of addresses in the address pool.
end-ip	Ending IP address that defines the range of addresses in the address pool.
prefix-length *prefix-length*	Specifies the number that indicates how many bits of the address is dedicated for the network.

Command Default

No pool of addresses is defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE, see ip nat pool command.

Examples

The following example shows how to translate between inside hosts addressed from one network to a globally unique network:

```
ip nat pool net-208 10.0.0.0 10.255.255.254 prefix-length 28
ip nat inside source list 1 pool net-208
!
interface ethernet 0
 ip address 10.0.0.1 255.255.255.224
 ip nat outside
!
interface ethernet 1
 ip address 192.168.255.255 255.255.0.0
 ip nat inside
!
access-list 1 permit 192.168.0.0 255.240.0.0
access-list 1 permit 192.168.0.1 255.255.0.0
```

ip nat route vrf

To configure an IP NAT route, use the **ip nat route vrf** command in global configuration mode. To remove the IP NAT route, use the **no** form of this command.

ip nat route vrf { *vrf* | *route-prefix* | *prefix-mask* | **global** }

no ip nat route vrf { *vrf* | *route-prefix* | *prefix-mask* | **global** }

Syntax Description

vrf	Specifies the service VRF.
route-prefix	Specifies the route prefix.
prefix-mask	Specifies the route mask.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 17.3.1	Command qualified for use in Cisco SD-WAN Manager C

Usage Guidelines

This command can be used to configure an IP NAT route using device templates to route traffic from the service-side to the transport-side (VPN 0) interface that has NAT enabled.

This command can be used for DIA solution.

Example

The following example shows how to configure an IP NAT default route to route traffic from service-side to the transport-side (VPN 0) NAT-enabled interface.

```
Device(config)# ip nat route vrf 65529 0.0.0.0 0.0.0.0 global
```

ip nat service

To enable an application-level gateway (ALG) for NAT translations of embedded IP addresses and port numbers in the payload of a packet, use the **ip nat service** command in global configuration mode. To disable ALG processing of NAT translations of embedded IP addresses and port numbers in the payload of a packet, use the **no** form of this command.

ip nat service { **all-algs** | **dns** { **tcp** | **udp** } | **ftp** | **sip** { **tcp** | **udp** } **port** *port-number* }

no ip nat service

Syntax Description

all-algs	Enables global NAT ALG for translation of IP address and port information inside the payload of an application packet.
dns	Enables Domain Name System (DNS) processing with an ALG for either TCP or UPD.
tcp	Specifies the TCP protocol.
udp	Specifies the UDP protocol.
ftp	Enables FTP processing with an ALG.
sip	Enables Session Initiation Protocol (SIP) processing with an ALG for either TCP or UDP.
port *port-number*	Specifies the port other than the default port in the range from 1 to 65533.

Command Default

NAT ALG translation support is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This command was introduced.

Usage Guidelines

Enable NAT ALG globally prior to enabling NAT ALG per protocol.

Examples

The following example shows how to enable global NAT ALG globally:

```
Device(config)# ip nat service all-algs
```

The following examples show how to enable NAT ALG for DNS for either TCP or UDP protocols:

```
Device(config)# ip nat service dns tcp
```

```
Device(config)# ip nat service dns udp
```

The following example shows how to enable NAT ALG for FTP:

```
Device(config)# ip nat service ftp
```

The following example shows how to enable NAT ALG for SIP for either TCP or UDP with port 5060:

```
Device(config)# ip nat service sip tcp port 5060
```

```
Device(config)# ip nat service sip udp port 5060
```

Related Commands

Commands	Description
clear ip nat translations	Clears dynamic NAT translations from the translation table.
show ip nat translations	Displays active NAT translations.
show platform hardware qfp active feature nat datapath summary	Displays configured and operational data specific to NAT.

ip nat settings preserve-sdwan-ports

To configure source ports preservation for the known SD-WAN port range during NAT, use the **ip nat settings preserve-sdwan-ports** command in global configuration mode. To remove the port preservation, use the **no** form of the command.

ip nat settings preserve-sdwan-ports

no ip nat settings preserve-sdwan-ports

Syntax Description

This command has no arguments or keywords.

Command Default

NAT port preservation for the known SD-WAN ports is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	This command was introduced.

Usage Guidelines

You may remove all NAT mapping configuration before configuring port-preservation command to allow port-preservation to take effect (avoiding reboot).

If there are existing NAT mapping configurations, ensure that you reboot the device after configuring the **ip nat settings preserve-sdwan-ports** command to achieve the expected behavior. If not, add NAT mapping configurations after configuring the **ip nat settings preserve-sdwan-ports** command.

Use the **ip nat settings preserve-sdwan-ports** command to enable port preservation for the control traffic using SD-WAN known ports. This is enabled during the following conditions:

- Interface overload
- Loopback overload

Examples

The following example shows how to configure NAT port preservation capability:

```
Device(config)# ip nat settings preserve-sdwan-ports
```

ip nat translation (timeout)

To change the Network Address Translation (NAT) timeout, use the **ip nat translation** command in global configuration mode. To disable the timeout, use the **no** form of this command.

ip nat translation { **dns-timeout** | **syn-timeout** | **icmp-timeout** *max-entries* | **port-timeout** **tcp-timeout timeout udp-timeout** }
no ip nat translation { **dns-timeout** | **syn-timeout** | **icmp-timeout** *max-entries* | **port-timeout** **tcp-timeout timeout udp-timeout** }

Syntax Description

dns-timeout	Specifies that the timeout value applies to connections to the Domain Name System (DNS). The default is 60 seconds.
syn-timeout	Specifies that the timeout value applies to TCP flows immediately after a synchronous transmission (SYN) message that consists of digital signals that are sent with precise clocking. The default is 60 seconds.
icmp-timeout	Specifies the timeout value for Internet Control Message Protocol (ICMP) flows. The default is 60 seconds.
port-timeout	Specifies that the timeout value applies to the TCP/UDP port.
tcp-timeout	Specifies that the timeout value applies to the TCP port. Default is 86,400 seconds (24 hours).
timeout	Specifies that the timeout value applies to dynamic translations, except for overload translations. The default is 86,400 seconds (24 hours).
udp-timeout	Specifies that the timeout value applies to the UDP port. The default is 300 seconds (5 minutes).

Command Default

NAT translation timeouts are enabled by default.

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines When port translation is configured, each entry contains more information about the traffic that is using the translation, which gives you finer control over translation entry timeouts. Non-DNS UDP translations time out after 5 minutes, and DNS times out in 1 minute. TCP translations time out in 24 hours, unless a TCP Reset (RST) or a Finish (FIN) bit is seen on the stream, in which case they will time out in 1 minute.

For usage guidelines, see the Cisco IOS XE ip nat translation (timeout) command.

Examples The following example shows how to configure the router to cause UDP port translation entries to time out after 10 minutes (600 seconds):

```
Device# configure terminal
Device(config)# ip nat translation udp-timeout 600
```

ip nat translation max-entries

To specify the maximum number of network address translation entries stored by the router, use the **ip nat translation max-entries** command in global configuration mode. To restore the default number of NAT entries, use the **no** form of this command.

ip nat translation max-entries *max-entries*
no ip nat translation max-entries *max-entries*

Syntax Description

max-entries *max-entries*	(Optional) Specifies the maximum number (1-2147483647) of NAT-PT translation entries. Default is unlimited.

Command Default No maximum size is specified for the NAT table.

Command Modes Global configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines Before you configure a NAT rate limit, you must first classify the current NAT usage and determine the sources of requests for NAT translations. If a specific host, an ACL, or a VRF instance is generating an unexpectedly high number of NAT requests, the host may be the source of a virus or worm attack.

Once you have identified the source of excessive NAT requests, you can set a NAT rate limit that constrains a specific host, an ACL, or a VRF instance, or you can set a general limit for the maximum number of NAT requests allowed regardless of their source.

Example

The following example shows how to limit the maximum number of allowed NAT entries to 300:

```
ip nat translation max-entries 300
```

nat64 provisioning

To configure the Network Address Translation 64 (NAT64) Mapping and Port Address Encapsulation (MAP-E) domain and MAP-E parameters, use the **nat64 provisioning** command in global configuration mode and NAT64 provisioning configuration mode. To disable NAT64 provisioning, use the **no** form of the command.

nat64 provisioning { **mode jp01** | **address-resolution-server** { **2** | **6** *address-resolution-server-url password username* } **api-key** { **2** | **6** *api-key-id* } | **hostname** *hostname* | **rule-server** { *rule-server-url* | **2** | **6** | **request wait-time** *wait-time-value* | **service-prefix** *ipv6-prefix* | **tunnel** { **interface** *interface-type* | **source** *interface-type* } } | **version draft-ietf-softwire-map-03** }

no nat64 provisioning

Syntax Description

mode	Specifies the NAT64 MAP-E domain and enters the NAT64 provisioning configuration mode.
jp01	Specifies the NAT64 provisioning mode.
address-resolution-server 2 6 *address-resolution-server-url username password*	Specifies the URL of the address resolution server. Allows you to configure the username and password of the address resolution server. Specifies an encryption type (2 or 6) for encrypting the username and password of the address resolution server.
api-key 2 6 *api-key-id*	Specifies the NAT64 API key ID. Specifies an encryption type (2 or 6) for encrypting the API key ID.
hostname *hostname*	Specifies the hostname of the Domain Name System (DDNS). The hostname comes from the MAP-E rule server. **Note** In case you overwrite the hostname, you can specify a new hostname.

rule-server 2 6 request wait-time *wait-time-value*	Specifies the URL of the MAP-E rule server. Specifies an encryption type (2 or 6) for encrypting the rule server URL. You enter the rule server URL in clear text. The rule server URL is later encrypted in the output of the **show running-config** command. (Optional) Specifies the wait time in seconds after the MAP-E CE device receives the Dynamic Domain Name System (DDNS) response. The wait time is before the DDNS response is sent to the MAP-E rule server.
service-prefix *ipv6-prefix*	Specifies the IPv6 prefix of the address resolution server. **Note** The service prefix needs to match the IPv6 prefix of the MAP-E rule returned by the border router.
tunnel interface *interface-name interface-number*	Specifies the NAT64 provisioning tunnel.
source *interface-type interface-number*	Specifies the NAT64 tunnel source.
version draft-ietf-softwire-map-03	Specifies the version of the MAP-E specification.

Command Default

NAT64 provisioning is not enabled.

Command Modes

Global configuration (config) mode and NAT64 provisioning configuration mode (config-nat64-provisioning)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	This command was introduced.

Usage Guidelines

Use this command to configure a MAP-E domain and parameters for transporting IPv4 packets over an IPv6 network using IP encapsulation.

Example

The following example shows how to enable NAT64 provisioning and configure the MAP-E domain and parameters:

```
Device(config)# nat64 settings fragmentation header disable
Device(config)# nat64 route 0.0.0.0/0 GigabitEthernet1
Device(config)# nat64 settings v4 tos ignore
Device(config)# interface GigabitEthernet1
Device(config-if)# nat64 settings mtu minimum 1500
Device(config-if)# nat64 provisioning mode jp01
Device(config-nat64-provisioning)# address-resolution-server
http://2001:db8:b000:0:fe7f:6ee7:33db:5013/nic/update
Device(config-nat64-provisioning)# address-resolution-server password encypted-password
Device(config-nat64-provisioning)# address-resolution-server username encypted-username
Device(config-nat64-provisioning)# rule-server
http://admin:admin@2001:DB8:A000::1//mape-rule.json
```

```
Device(config-nat64-provisioning)# rule-server request wait-time 180
Device(config-nat64-provisioning)# hostname hostname
Device(config-nat64-provisioning)# tunnel interface Tunnel1
Device(config-nat64-provisioning)# tunnel source GigabitEthernet2
Device(config-nat64-provisioning)# service-prefix 2001:DB8:b800::/48
```

Related Commands

Commands	Description
nat64 route	Specify NAT64 prefix to which an IPv4 prefix should be translated.
nat64 settings	Configure NAT64 settings.
nat64 settings mtu	Configure the path maximum transmission unit (MTU) size for preventing fragmentation of IPv4 packets for translation to IPv6.

nat64 route

To specify the Network Address Translation 64 (NAT64) prefix to which an IPv4 prefix should be translated, use the **nat64 route** command in global configuration mode. To disable the configuration, use the **no** form of this command.

nat64 route { *ipv4-prefix/ mask interface-type interface-number* }
no nat64 route *ipv4-prefix/ mask*

Syntax Description

ipv4-prefix / *mask*	Length of the IPv4 prefix and the mask.
interface-type	Interface type. For more information, use the question mark (?) online help.
interface-number	Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.

Command Default

No NAT64 routing is performed.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	This command was introduced.

Usage Guidelines

A prefix that is configured on an interface is used as the stateless prefix on that interface. If no interface-specific prefix is configured, the configured global prefix is used for NAT64 translation.

For usage guidelines, see the Cisco IOS XE nat64 route command.

Example

The following example shows how to assign an IPv4 prefix and mask to an interface:

```
Device(config)# nat64 route 0.0.0.0/0 GigabitEthernet1
```

Related Commands

Commands	Description
nat64 provisioning	Configure the Mapping and Port Address Encapsulation (MAP-E) domain and parameters.
nat64 settings	Configure NAT64 settings.
nat64 settings mtu	Configure MTU size for preventing fragmentation of IPv4 packets for translation to IPv6 using NAT64.

nat64 settings

To configure Network Address Translation 64 (NAT64) settings, use the **nat64 settings** command in global configuration mode. To disable NAT64 settings, use the **no** form of this command.

nat64 settings { **fragmentation header disable** | **v4 tos ignore** }
no nat64 settings { **fragmentation header disable** | **v4 tos ignore** }

Syntax Description

fragmentation header disable	Disables the NAT64 fragmentation header.
v4 tos ignore	Specifies not to copy the IPv4 type-of-service (ToS) header.

Command Default

NAT64 settings are disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	This command was introduced.

Usage Guidelines

By default, NAT64 adds a fragmentation header for all IPv4-to-IPv6 packets that do not have the Do Not Fragment (DF) bits set. Configure the **nat64 settings fragmentation header disable** command to disable the adding of a fragmentation header for packets that are not fragmented.

By default, NAT64 copies ToS bits from an IPv4 header to an IPv6 header. Configure the **nat64 settings v4 tos ignore** command to disable the copying of ToS bits from an IPv4 header to an IPv6 header.

Example

The following example shows how to disable the NAT64 fragmentation header:

```
Router(config)# nat64 settings fragmentation header disable
```

Related Commands

Commands	Description
nat64 provisioning	Configure the Mapping and Port Address Encapsulation (MAP-E) domain and parameters.
nat64 settings mtu	Configure MTU size for preventing fragmentation of IPv4 packets for translation to IPv6 using NAT64.

nat64 settings mtu

To configure the path maximum transmission unit (MTU) size for preventing fragmentation of IPv4 packets for translation to IPv6 using Network Address Translation (NAT64), use the **nat64 settings mtu** command in interface configuration mode. To disable the MTU size for NAT64, use the **no** form of this command.

nat64 settings mtu minimum *mtu-value*
no nat64 settings mtu

Syntax Description

minimum *mtu-value*	MTU size in bytes.

Command Default

NAT64 MTU size is not set.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	Additional parameter qualified: **mtu**.

Usage Guidelines

Path maximum transmission unit (MTU) discovery prevents fragmentation in the path between endpoints. Path MTU discovery is used to dynamically determine the lowest MTU along the path from a packet's source to its destination. Path MTU discovery is supported only by TCP and UDP. Path MTU discovery is mandatory in IPv6, but it is optional in IPv4. IPv6 devices never fragment a packet—only the sender can fragment packets.

Example

The following example shows how to set the MTU size for NAT64:

```
Router(config)# interface GigabitEthernet1
Router(config-if)# nat64 settings mtu minimum 1500
```

Related Commands

Commands	Description
nat64 settings	Configure NAT64 settings.

nat64 translation timeout tcp

To configure a NAT64 translation timeout value for TCP traffic, use **nat64 translation timeout tcp** command in global configuration mode. To remove the configuration, use the **no** form of this command.

nat64 translation timeout tcp { *time* | **never** }

no nat64 translation timeout tcp { *time* | **never** }

Syntax Description

time	Specifies the timeout value. Range: 0 to 536870 seconds.
never	Specifies that TCP translation never expires.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 17.3.1	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

This command can be used to configure a NAT64 translation timeout value for TCP traffic.

Example

The following example shows how to configure a NAT64 translation timeout value for TCP traffic to 30 seconds.

```
Device(config)# nat64 translation timeout tcp 30
```

nat64 translation timeout udp

To configure a NAT64 translation timeout value for UDP traffic, use the **nat64 translation timeout udp** command in global configuration mode. To remove the configuration, use the **no** form of this command.

nat64 translation timeout udp { *time* | **never** }

no nat64 translation timeout udp { *time* | **never** }

Syntax Description

time	Specifies the timeout value. Range: 0–536870 seconds.
never	UDP translation never expires.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 17.3.1	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

This command can be used to configure a NAT64 translation timeout value for UDP traffic.

Example

The following example shows how to configure a NAT64 translation timeout value for UDP traffic to two seconds.

```
Device(config)# nat64 translation timeout udp 2
```

nat66 max vpn

To configure the maximum number of virtual routing and forwarding (VRF) connections allowed for prefix translation, use the **nat66 max-vpn** command in global configuration mode. To remove the maximum number of VRFs allowed for prefix translation, use the **no** form of this command.

nat66 max-vpn *number*

no nat66 max-vpn

Syntax Description

max-vpn *number*	Specifies the maximum number of VRF connections allowed for prefix translation. The maximum number of VRFs allowed is 250.

Command Default

The maximum number of VRF connections are not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

When using prefix delegation (PD) with NAT66, an outside prefix is extended by adding a VRF ID to the prefix translation. An inside prefix length of /64 and a PD prefix length of /56 results in /56 + 8 bits of a VRF ID for an outside prefix length.

Examples

The following example shows how to configure the maximum number of VRFs allowed for prefix translation:

```
Device(config)# nat66 max-vpn number
```

nat66 outside

To configure a NAT66 outside network interface for prefix translation, use the **nat66 outside** command in interface configuration mode. To remove the NAT66 outside network address prefix, use the **no** form of this command.

nat66 outside

no nat66 outside

Syntax Description

This command has no arguments or keywords.

Command Default

No NAT66 outside network interface is configured for prefix translation.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE nat66 outside command.

Examples

The following example shows how to configure a NAT66 outside network interface:

```
Device(config-if)# nat66 outside
```

nat66 prefix

To configure translation of an inside and an outside IPv6 source address prefix for NAT66 translation, use the **nat66 prefix** command in global configuration mode. To remove the IPv6 prefix from the IPv6 prefix translation, use the **no** form of this command.

nat66 prefix inside *prefix/prefix-length* **outside** *prefix/prefix-length* **interface** *interface-type interface-number* **vrf** *vrf-id* **egress-interface** *interface-type interface-number*

no nat66 prefix inside *prefix/prefix-length* **outside** *prefix/prefix-length* **interface** *interface-type interface-number* **vrf** *vrf-id* **egress-interface** *interface-type interface-number*

Syntax Description

inside	Specifies the IPv6 inside network.
outside	Specifies the IPv6 outside network.
prefix	The IPv6 network prefix.
prefix-length	The length of the IPv6 address prefix.

interface *interface-type interface-number*	Specifies the outside interface type and interface number that are automatically assigned global IPv6 addresses by Stateless Address Autoconfiguration (SLAAC) for forwarding packets.
vrf *vrf-id*	Specifies the VRF and VRF ID used for prefix translation.
egress-interface *interface-type interface-number*	(Optional) Specifies the egress interface type and the egress interface number that are used for forwarding packets to the internet-facing or WAN interface.

Command Default

No prefix translations are configured for an inside or an outside IPv6 source address.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	This command was modified. Added the **egress-interface** type keyword to configure multiple WAN links for NAT66 DIA.
Cisco IOS XE Catalyst SD-WAN Release 17.13.1a	This command was modified. Added the **interface** keyword to configure the outside interface type and interface-number for NAT66 DIA translations by Stateless Address Autoconfiguration (SLAAC).

Usage Guidelines

For usage guidelines, see the Cisco IOS XE nat66 prefix command.

Examples

The following example shows how to configure IPv6-to-IPv6 address prefix translation:

```
Device(config)# nat66 prefix inside 2001:DB8:A14:18::/80 outside 2001:DB8:A1:F::/80 vrf 1
```

The following example shows how to configure NAT66 DIA with two interfaces, GigabitEthernet1 and GigabitEthernet4:

```
interface GigabitEthernet1
 no shutdown
 ipv6 address 2001:a1:f::f/64
 ipv6 nd ra suppress all
 no mop enabled
 no mop sysid
 negotiation auto
 nat66 outside
!
interface GigabitEthernet4
 no shutdown
 ipv6 address 2001:a0:14::f/64
 ipv6 enable
 ipv6 nd ra suppress all
 no mop enabled
 no mop sysid
 negotiation auto
 nat66 outside
!
```

```
nat66 prefix inside 2001:a14:18:0::/64 outside 2001:a1:f::/64 vrf 1 egress-interface
GigabitEthernet1
nat66 prefix inside 2001:a14:18:0::/64 outside 2001:a0:14::/64 vrf 1 egress-interface
GigabitEthernet4
nat66 prefix inside FC00:1:2:3::/80 outside 3001:a1:5::/80 vrf 100
nat66 route vrf 1 2001:a0:5::/64 global
nat66 route vrf 100 ::/0 global
```

The following example shows how to configure Stateless Address Autoconfiguration (SLAAC) to automatically assign IPv6 addresses for NAT66 prefix translations:

Enable NAT66 outside network interface on the NAT66 DIA WAN interface:

```
interface GigabitEthernet1
  nat66 outside
```

Enable automatic configuration of IPv6 address on the NAT66 DIA WAN interface:

```
interface GigabitEthernet1
 ipv6 address autoconfig
 ipv6 enable
 ipv6 nd autoconfig default-route
```

Create SLAAC mapping translation rules with the NAT66 DIA WAN interface:

```
nat66 prefix inside 2001:a0:5::/64 outside interface GigabitEthernet1 vrf 1
nat66 prefix inside 2001:a0:5::/64 outside interface GigabitEthernet1
```

For more information about configuring SLAAC to automatically assign IPv6 addresses for NAT66 prefix translations, see the section *Configure NAT66 DIA Using Stateless DHCP* in *How NAT66 DIA Works*.

nat66 route vrf

To configure a NAT66 VRF route, use the **nat66 route vrf** command in global configuration mode. To disable the configuration of a NAT66 VRF route, use the **no** form of this command.

nat66 route vrf *vrf-name ipv6-dest-prefix* **global**

no nat66 route vrf *vrf-name ipv6-dest-prefix* **global**

Syntax Description

vrf	Specifies all the virtual private network (VPN) VRF tables or a specific VRF table for IPv6 addresses.
vrf-name	The name of a specific VRF table for an IPv6 address.
ipv6-dest-prefix	The IPv6 destination prefix.
global	Specifies the globally routable prefix.

Command Default

No NAT66 VRF route is configured.

Command Modes

Global configuration (config)

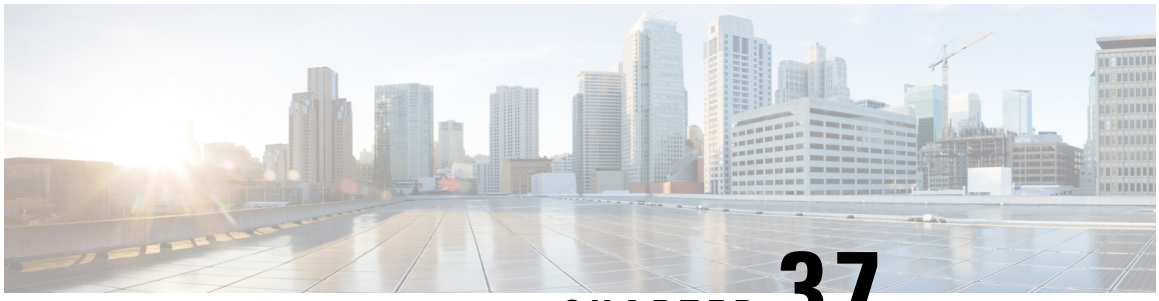
Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Examples

The following example shows how to configure the NAT66 VRF route:

```
Device(config)# nat66 route vrf 1 2001:DB8:A14:19::/64 global
Device(config)# nat66 route vrf 1 2001:DB8:3D0:1::/64 global
```



CHAPTER 37

NTP Commands

- ntp access-group, on page 509
- ntp authentication-key, on page 510
- ntp server, on page 511
- ntp source, on page 512
- ntp trusted-key, on page 512

ntp access-group

To control access to Network Time Protocol (NTP) services on the system, use the **ntp access-group** command in global configuration mode. To remove access control to the NTP services, use the **no** form of this command.

ntp access-group { **peer** *access-list-number* }
no ntp access-group { **peer** *access-list-number* }

Syntax Description

peer	Allows time requests and NTP control queries and permits the system to synchronize with the remote system.
access-list-number	Number (from 1 to 9199) of a standard IPv4 access list.

Command Default

By default, there is no access control. Full access is granted to all systems.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE, ntp access-group command.

Examples

The following example shows how to configure a system to allow itself to be synchronized by a peer:

```
Router(config)# ntp access-group peer 25
```

The following example shows how to remove all the configured NTP options and disable the NTP server:

```
Router(config)# no ntp
```

ntp authentication-key

To define an authentication key for Network Time Protocol (NTP), use the **ntp authentication-key** command in global configuration mode. To remove the authentication key for NTP, use the **no** form of this command.

ntp authentication-key *number* **md5** *key*
no ntp authentication-key *number*

Syntax Description

number	Key number from 1 to 4294967295.
md5	Specifies the authentication key. Message authentication support is provided using the message digest 5 (MD5) algorithm. The key type **md5** is the only key type supported.
key	Character string of up to 32 characters that is the value of the MD5 key. **Note** In auto secure mode, an error is displayed on the console and the authentication key is not configured if the character string length exceeds 32.

Command Default

No authentication key is defined for NTP.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE, ntp authentication-key command.

Examples

The following example shows how to configure the system to synchronize only to systems providing the authentication key in their NTP packets:

```
Router(config)# ntp authentication-key 65535 md5 test
```

The following example shows how to remove all the configured NTP options and disable the NTP server:

```
Router(config)# no ntp
```

ntp server

To configure a router to allow its software clock to be synchronized with the software clock of a Network Time Protocol (NTP) time server, use the **ntp server** command in global configuration mode. To disable this capability, use the **no** form of this command.

ntp server { *ip-address* } [**source** *interface-type*] [**key** *key-id*] [**prefer** **version** *version*]
no ntp server { *ip-address* }

Syntax Description

ip-address	IPv4 address of the NTP peer providing or being provided the software clock synchronization.
version	(Optional) Defines the NTP version number.
number	(Optional) NTP version number. The range is from 2 to 4. **Note** In Cisco IOS Release 12.2SX, the number range is from 1 to 4.
key	(Optional) Specifies the authentication key.
key-id	(Optional) Authentication key to use when sending packets to this NTP peer.
source	(Optional) Specifies that the source address must be taken from the specified interface.
interface-type	(Optional) Name of the interface from which to pick the IPv4 or IPv6 source address. For more information, use the question mark (?) online help function. It is a parser error if the interface is not pre-configured.
prefer	(Optional) Makes this NTP peer the preferred peer that provides the clock synchronization.

Command Default

No servers are configured by default. When a server is configured, the default NTP version number is 3, an authentication key is not used, and the source IPv4 is taken from the outgoing interface.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE, ntp server command.

Examples

The following example shows how to configure a router to allow its software clock to be synchronized with the software clock of an NTP server by using the device at the IPv4 address:

```
Router(config)# ntp server 10.0.1.1 source GigabitEthernet8 key 65535 prefer version 4
```

ntp source

To use a particular source address in Network Time Protocol (NTP) packets, use the **ntp source** command in global configuration mode. To remove the specified source address, use the **no** form of this command.

ntp source *interface-type interface-number*
no ntp source

Syntax Description

interface-type	Type of interface.
interface-number	Number of the interface.

Command Default

Source address is determined by the outgoing interface.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE, ntp source command.

Examples

The following example shows how to configure a router to use the IPv4 or IPv6 address of GigabitEthernet interface 8 as the source address of all outgoing NTP packets:

```
Router(config)# ntp source GigabitEthernet 8
```

The following example shows how to remove all the configured NTP options and disable the NTP server:

```
Router(config)# no ntp
```

ntp trusted-key

To authenticate the identity of a system to which Network Time Protocol (NTP) will synchronize, use the **ntp trusted-key** command in global configuration mode. To disable the authentication of the identity of the system, use the **no** form of this command.

ntp trusted-key *key-number*
no ntp trusted-key *key-number*

Syntax Description

key-number	Specifies the key number of the authentication key to be trusted. Valid values are from 1 to 65535.

Command Default

Authentication of the identity of the system is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE, ntp trusted-key command.

Configure the trusted key with the key number of the configured authentication-key to have a successful authentication.

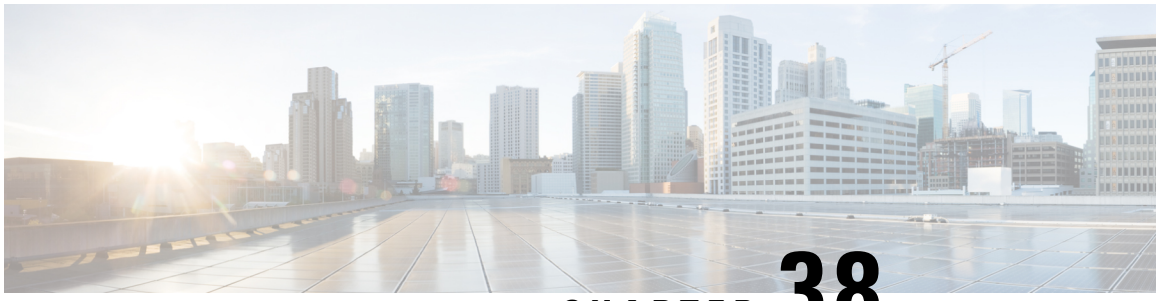
Examples

The following example shows how to configure the system to synchronize only to systems providing authentication keys in their NTP packets:

```
Router(config)# ntp authentication-key 65535 md5 test
Router(config)# ntp trusted-key 65535
```

The following example shows how to remove all the configured NTP options and disable the NTP server:

```
Router(config)# no ntp
```



CHAPTER 38

Object-Group Commands

- continent, on page 515
- country, on page 516
- description (fqdn-group), on page 517
- description (geo-group), on page 517
- geo database, on page 518
- geo database revert, on page 519
- geo database update, on page 519
- group-object (fqdn-group), on page 520
- group-object (geo-group), on page 521
- object-group fqdn, on page 521
- object-group geo, on page 522
- object-group network, on page 523
- object-group security, on page 524
- object-group service, on page 525
- pattern, on page 526

continent

To add a continent to a geo object group, use the **continent** command in configuration geo group mode. To remove a continent from a geo object group, use the **no** form of this command.

continent *continent-code*

no continent *continent-code*

Syntax Description

continent *continent-code*	Specifies the two-letter continent codes: • **AF**: Africa • **AN**: Antarctica • **AS**: Asia • **EU**: Europe • **NA**: North America • **OC**: Oceania • **SA**: South America

Command Default

No continent is added to a geo object group.

Command Modes

Configuration geo group (config-geo-group)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

When you configure the **object-group geo** command, the command mode changes to geo group configuration mode (config-geo-group), which allows you to add a continent to a geo object group.

Examples

The following example shows how to add the continent EU to a geo object group:

```
Device(config-geo-group)# continent EU
```

country

To configure a country in a geo object group, use the **country** command in configuration geo group mode. To remove a country from a geo object group, use the **no** form of this command.

country *country-code*

no country *country-code*

Syntax Description

country *country-code*	Specifies the three-letter ISO-3166 country codes.

Command Default

No country is added to a geo object group.

Command Modes

Configuration geo group (config-geo-group)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

When you configure the **object-group geo** command, the command mode changes to geo group configuration mode (config-geo-group), which allows you to configure a country for a geo object group.

Examples

The following example shows how to add the country GBR to a geo object group:

```
Device(config-geo-group)# country GBR
```

description (fqdn-group)

To add a description to an object group, use the **description** command in fqdn group configuration mode. To remove a description from an object group, use the **no** form of this command.

description *description-text*

no description *description-text*

Syntax Description

description *description-text*	Specifies a description for a fully qualified domain name (FQDN) object group. You can use up to 200 characters.

Command Default

No description is added to an FQDN object group.

Command Modes

fqdn group configuration mode (config-fqdn-group)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

When you configure the **object-group fqdn** command, the command mode changes to fqdn group configuration mode (config-fqdn-group), which allows you to add a description to an FQDN object.

Examples

The following example shows how to add a description to an FQDN object group:

```
Device(config-fqdn-group)# description Source FQDN
```

description (geo-group)

To add a description to an object group, use the **description** command in geo group configuration mode. To remove a description from an object group, use the **no** form of this command.

description *description-text*

no description *description-text*

Syntax Description

description *description-text*	Specifies a description for a geo object group. You can use up to 200 characters.

Command Default

No description is added to a geo object group.

Command Modes

geo group configuration mode (config-geo-group)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

When you configure the **object-group geo** command, the command mode changes to geo group configuration mode (config-geo-group), which allows you to add a description to a geo object.

Examples

The following example shows how to add a description to a geo object group:

```
Device(config-geo-group)# description GEO_1
```

geo database

To enable a geo database, use the **geo database** command in global configuration mode. To remove a geo database from the configuration, use the **no** form of this command.

geo database

no geo database

Syntax Description

This command has no arguments or keywords.

Command Default

A geodatabase is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

After executing the **geo database** command, you must commit your changes to enable the geolocation database.

Examples

The following example shows how to configure the **geo database** command:

```
Device(config)# geo database
```

The following is a sample output from the **show geo status** command.

```
Device# show geo status
Geo-Location Database is enabled
File in use       : Device default
```

geo database revert

To revert the geolocation database file back to the default if the geolocation database is corrupted, use the **geo database revert** command in privileged EXEC mode.

geo database revert default

Syntax Description This command has no arguments or keywords.

Command Default The geolocation database file is not reverted to the default.

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines Use the **geo database revert** command to revert the geolocation database file to its default if the geolocation database is corrupted.

Examples

The following example shows a sample output from the **geo database revert default** command:

```
Device# geo database revert default
```

geo database update

To update the geolocation database file, use the **geo database update** command in privileged EXEC mode.

geo database update file [**bootflash:** | **crashinfo:** | **flash:**]

Syntax Description

file	Specifies the full directory path to the geolocation database file within one of the following folders: • bootflash **Note** The default file location for the geodatabase is in the bootflash folder. • crashinfo • flash

Command Default

The geolocation database is not updated.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

To ensure that you are using up-to-date geographical location data, we recommend that you update the geolocation database.

Examples

The following example shows how to update the geo database in the bootflash folder:

```
Device# geo database update bootflash:geo_ip4_db
```

group-object (fqdn-group)

To view existing fully qualified domain name (FQDN) objects, or to create a new FQDN object, use the **group-object** command in configuration fqdn group mode. To remove an FQDN group object, use the **no** form of this command.

group-object *group-object-name*

no group-object *group-object-name*

Syntax Description

group-object *group-object-name*	Displays the existing FQDN objects you previously created. You can also create a new FQDN object.

Command Default

No group object is displayed or created.

Command Modes

Configuration fqdn group (config-fqdn-group)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

You can view existing FQDN objects, or you can create a new FQDN object using the **group-object** command.

Examples

The following example shows how to create a group object called FQDN-1:

```
Device(config-fqdn-group)# group-object FQDN-1
```

group-object (geo-group)

To view existing geo objects, or to create a new geo object, use the **group-object** command in configuration geo group mode. To remove a group object, use the **no** form of this command.

group-object *group-object-name*

no group-object *group-object-name*

Syntax Description

group-object *group-object-name*	Specifies an existing geo object (child) to be included in the current object group (parent).

Command Default

No group object is added to a geo object group.

Command Modes

Configuration geo group (config-geo-group)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

You can create nested geo objects using the **group-object** command.

Examples

The following example shows how to create a geo object called GEO_1:

```
Device(config-geo-group)# group-object GEO_1
```

object-group fqdn

To create a fully-qualified domain name (FQDN) object group for use in object-group-based access control lists (ACLs), use the **object-group fqdn** command in global configuration mode. To remove an FQDN object group from the configuration, use the **no** form of this command.

object-group fqdn *object-group-name*

no object-group fqdn *object-group-name*

Syntax Description

object-group-name	Specifies the name of a FQDN object group. A sequence of 1 to 64 characters consisting of letters, digits, underscores (_), dashes (-), or periods. The *object-group-name* must start with a letter.

Command Default

No FQDN object group is created.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

When Access Control Lists (ACLs) are configured using an FQDN, ACLs can be applied based on the destination domain name. The destination domain name is then resolved to an IP address, which is provided to the client as part of the DNS response.



Note When defining a firewall rule in a security policy, avoid configuring an **fqdn** in both the source data prefix and the destination data prefix in the same firewall rule.

Create two different rules containing the following:

- 1st rule: Use **fqdn** in the source data prefix only.
- 2nd rule: Use **fqdn** in the destination data prefix only.

Examples

The following example shows how to create a new FQDN object group, obj.example.com:

```
Device (config)# object-group obj.example.com
object-group fqdn TEST
pattern ".*\.cisco\.com" "test.cisco.com" and "test.test.cisco.com"
object group obj-talosintelligence.com
 fqdn talosintelligence.com id 268434436
```

object-group geo

To create a geolocation object group for use in object group-based access control lists (ACLs), use the **object-group geo** command in global configuration mode. To remove a geolocation object group from the configuration, use the **no** form of this command.

object-group geo *object-group-name*

no object-group geo *object-group-name*

Syntax Description

object-group-name	Specifies the name of the geo object group. A sequence of 1 to 64 characters consisting of letters, digits, underscores (_), dashes (-), or periods. The *object-group-name* must start with a letter.

Command Default

No geolocation object group is created.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Add object groups to use in Access Control Lists (ACLs) to enable geolocation-based firewall rules.

Note When defining a firewall rule in a security policy, avoid configuring a **geo** in both the source data prefix and the destination data prefix in the same firewall rule.

Create two different rules containing the following:

- 1st rule: Use **geo** in the source data prefix only.
- 2nd rule: Use **geo** in the destination data prefix only.

Examples

The following example shows how to create a new object group GEO_1:

```
Device(config)# object-group geo GEO_1
```

object-group network

To define network object groups for use in object group-based access control lists (ACLs) and enter network group configuration mode, use the **object-group network** command in global configuration mode. To remove network object groups from the configuration, use the **no** form of this command.

object-group network *object-group-name*
no object-group network *object-group-name*

Syntax Description

object-group-name	Name for a network type of object group. *object-group-name* is a sequence of 1 to 64 characters consisting of letters, digits, underscores (_), dashes (-), or periods (.). The *object-group-name* must start with a letter.

Command Default

No network object groups are created.

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines When you configure the **object-group network** command, the command mode changes to network group configuration mode (config-network-group) and allows you to populate or modify a network object-group ACL. The following command is available in network group configuration mode:

host {*host-address*}—Specifies the host object. You must use an IPv4 address for the host address.

Note the following restrictions:

- You cannot associate an empty object group with an access control list (ACL).
- If you use an object group with an ACL, you cannot empty or delete the object group. You can use Cisco SD-WAN Manager add-on feature templates to delete an attached ACL and its object group in the same template push, as long as there are no other references to the object group in the configuration. However, the commands will fail on the device. To avoid this, do not delete or empty an object group that is associated with an ACL.

For further usage guidelines, see the Cisco IOS XE `object-group network` command.

Examples

```
object-group network Auth-Servers
 host 10.16.137.22
 !
```

object-group security

To create an object group to identify the traffic coming from a specific user or endpoint, use the **object-group security** command in global configuration mode. To remove the object group, use the **no** form of this command.

object-group security *name*

no object-group security *name*

Syntax Description

name	Object group name.

Command Default No object group is defined.

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `object-group security` command.

Examples

The following example shows how the **object-group security** command is used in the class map configuration of the Security Group Access (SGA) zone-based firewall:

```
Device(config)# object-group security myobject1
Device(config-object-group)# security-group tag-id 1
Device(config-object-group)# exit
Device(config)# class-map type inspect xmatch-any myclass1
Device(config-cmap)# match group-object security source myobject1
Device(config-cmap)# end
```

object-group service

To define service object groups for use in object-group-based access control lists (ACLs), use the **object-group service** command in global configuration mode. To remove service object groups from the configuration, use the **no** form of this command.

object-group service *object-group-name*
no object-group service *object-group-name*

Syntax Description

object-group-name	Name of a service type of object group.

Command Default

No service object groups are created.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

When you configure the **object-group service** command, configuration mode changes to service group configuration mode (config-service-group) allows you to populate or modify a service-object-group ACL. The following commands are available in service group configuration mode:

- {**tcp** | **udp** | **tcp-udp**} [**source** {*source-port-number* | **range** *minimum-port maximum-port*}] [*destination-port-number* | **range** *minimum-port maximum-port*]—Specifies a TCP or UDP protocol port number or a range of port numbers.
- **ip**—Specifies any protocol.
- *number*— Specifies a specific protocol number
- **icmp**—Specifies the ICMP protocol.

Note the following restrictions:

- You cannot associate an empty object group with an access control list (ACL).

- If you use an object group with an ACL, you cannot empty or delete the object group. You can use Cisco SD-WAN Manager add-on feature templates to delete an attached ACL and its object group in the same template push, as long as there are no other references to the object group in the configuration. However, the commands will fail on the device. To avoid this, do not delete or empty an object group that is associated with an ACL.

For more usage guidelines, see the Cisco IOS XE `object-group service` command.

Examples

```
object-group service ZBF-DIA-External
 tcp 80
 udp
 tcp range 1024 65535
 tcp source 23
 ip
 icmp
!
```

pattern

To add a pattern for finding valid fully qualified domain names (FQDN), use the **pattern** command in fqdn group configuration mode. To remove a pattern from the configuration, use the **no** form of this command.

pattern *match-pattern*

no pattern *match-pattern*

Syntax Description

match-pattern	Specifies a pattern for finding valid FQDNs.

Command Default

No pattern is matched.

Command Modes

fqdn group configuration mode (config-fqdn-group)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

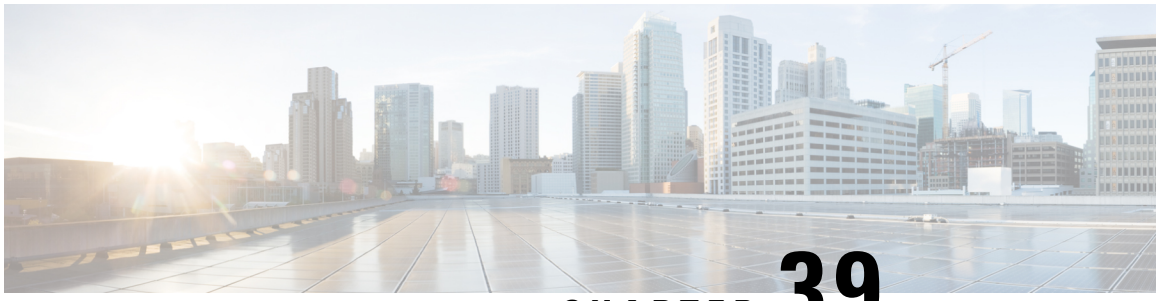
Usage Guidelines

When you configure the **object-group fqdn** command, the command mode changes to fqdn group configuration mode (config-fqdn-group), which allows you to add a pattern for finding valid FQDNs.

Examples

The following example shows how to add a pattern of example.com:

```
Device(config-fqdn-group)# pattern example.com
```



CHAPTER 39

OMP Commands

- advertise, on page 527
- distance , on page 529
- ecmp-limit (omp), on page 529
- graceful-restart (omp), on page 530
- no shutdown (omp), on page 531
- omp, on page 532
- outbound tloc-color, on page 533
- overlay-as (omp), on page 534
- send-path-limit (omp), on page 535
- timers, on page 536
- tloc-color-compatibility, on page 538

advertise

To advertise additional paths for a BGP peer policy template based on the best path selection, use the **advertise** command in address family configuration mode at the specific VPN or VRF level.

Route advertisements that you configure with the **advertise** command apply to all VPNs configured on the router. The advertise command can be issued for either a VPN, or for all VPNs on a device.

advertise [**bgp**] [**connected**] [**ospf** *type*] [**static**]

no advertise [**bgp**] [**connected**] [**ospf** *type*] [**static**]

Syntax Description

bgp	BGP Routes: Advertise all BGP routes learned by the Cisco IOS XE Catalyst SD-WAN devices to OMP.
connected	Connected Routes: Advertise all connected routes on the Cisco IOS XE Catalyst SD-WAN devices to OMP. The connected routes are advertised by default. To disable advertisement, use the **no advertise connected** command.

ospf *type*	OSPF Routes: Advertise all OSPF routes learned by the local Cisco IOS XE Catalyst SD-WAN devices to OMP. For the global OMP configuration, *type* can be **external**, to advertise routes learned from external ASs. For the VPN-specific OMP configuration, *type* can be **external**, to advertise routes learned from the local AS. For the global OMP configuration, OSPF external routes are advertised by default.
static	Static Routes: Advertise all static routes configured on the Cisco IOS XE Catalyst SD-WAN devices to OMP. Static routes are advertised by default. To disable advertisement, use the **no advertise static** command.

Command Default

This command has no default behavior.

Command Modes

OMP configuration (config-omp)

Address family configuration (config-af)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Example

The following example shows how to advertise to Cisco Catalyst SD-WAN Controller, the routes that a Cisco IOS XE Catalyst SD-WAN device has learned from the local network in a branch network that is running static, connected, and OSPF protocols.

```
config-transaction
sdwan
omp
address-family ipv4
advertise static
advertise connected
advertise ospf external
```

Advertise routes to OMP:

```
show running-config vpn 1
omp
 no shutdown
 graceful-restart
distance 100
 timers
  holdtime 15
  graceful-restart-timer 120
 exit
 advertise static
 advertise connected
 advertise ospf external
!
```

distance

To configure the OMP administrative distance, use the **distance** command in router configuration mode or address-family configuration mode. To reset the value to its defaults, use the **no** form of this command.

distance *kilometers*
no distance

Syntax Description

kilometers	Administrative distance for OMP routes. The Cisco vSmart Controllers learn the topology of the overlay network and the services available in the network using OMP routes. The distance can be a value between 1–255.

Command Default

The default administrative distances are based on a protocol.

Command Modes

OMP configuration (config-omp)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Examples

The following example shows how to set the OMP administrative distance to 165:

```
Device# config-transaction
Device(config)# sdwan
Device(config-sdwan)# omp
Deviced(config-omp)# distance 165
```

ecmp-limit (omp)

To configure the maximum number of OMP paths that can be installed in the vEdge router's route table (on vEdge routers only), use the **ecmp-limit** command in OMP configuration mode. To remove the maximum number of OMP routes that can be installed in the vEdge router's route table, use the **no** form of this command.

ecmp-limit *number-of-paths*
no ecmp-limit *number-of-paths*

Syntax Description

number-of-paths	Maximum number of OMP paths that can be installed in the vEdge router's route table. Each TLOC consists of a IP address and color. You can specify between 1 to 16 routes.

Command Default

4 paths are advertised.

Command Modes

OMP configuration (config-omp)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Examples

The following example shows how to configure OMP on a router:

```
sdwan
 omp
  no shutdown
  overlay-as 4294967295
  send-path-limit 16
  ecmp-limit 16
  graceful-restart
  no as-dot-notation
  timers
   holdtime 65535
   advertisement-interval 65535
   graceful-restart-timer 43200
   eor-timer 3600
  !
  address-family ipv4
   advertise bgp
   advertise ospf external
   advertise connected
   advertise static
   advertise eigrp
   advertise lisp
   advertise isis
  !
  address-family ipv6
   advertise bgp
   advertise connected
   advertise static
   advertise eigrp
   advertise lisp
   advertise isis
```

graceful-restart (omp)

To control graceful restart for OMP, use the **graceful-restart** command in OMP configuration mode. To remove graceful restart for OMP, use the **no** form of this command.

graceful-restart
no graceful-restart

Command Default

Graceful restart for OMP is enabled on all routers.

Command Modes

OMP configuration (config-omp)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Examples

The following example shows how to configure OMP on a router:

```
sdwan
 omp
  no shutdown
  overlay-as 4294967295
  send-path-limit 16
  ecmp-limit 16
  graceful-restart
  no as-dot-notation
  timers
   holdtime 65535
   advertisement-interval 65535
   graceful-restart-timer 43200
   eor-timer 3600
  !
  address-family ipv4
   advertise bgp
   advertise ospf external
   advertise connected
   advertise static
   advertise eigrp
   advertise lisp
   advertise isis
  !
  address-family ipv6
   advertise bgp
   advertise connected
   advertise static
   advertise eigrp
   advertise lisp
   advertise isis
```

no shutdown (omp)

To enable OMP on a router, use the **no shutdown** command in OMP configuration mode. To disable OMP on a router, use **shutdown**.

no shutdown
shutdown

Command Default

OMP is enabled by default on all routers.

Command Modes

OMP configuration (config-omp)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Examples

The following example shows how to configure OMP on a router:

```
sdwan
```

```
omp
 no shutdown
 overlay-as 4294967295
 send-path-limit 16
 ecmp-limit 16
 graceful-restart
 no as-dot-notation
 timers
  holdtime 65535
  advertisement-interval 65535
  graceful-restart-timer 43200
  eor-timer 3600
 !
 address-family ipv4
  advertise bgp
  advertise ospf external
  advertise connected
  advertise static
  advertise eigrp
  advertise lisp
  advertise isis
 !
 address-family ipv6
  advertise bgp
  advertise connected
  advertise static
  advertise eigrp
  advertise lisp
  advertise isis
```

omp

To configure Cisco SD-WAN Overlay Management Protocol (OMP) for a router, use the **omp** command in SD-WAN configuration mode. To remove OMP configuration from a router, use the **no** form of this command.

omp
no omp

Command Default

OMP is enabled on all Cisco Catalyst SD-WAN routers and Cisco Catalyst SD-WAN Controllers.

Command Modes

SD-WAN configuration (config-sdwan)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Examples

The following example shows how to configure OMP on a router:

```
sdwan
 omp
  no shutdown
  overlay-as       4294967295
  send-path-limit  16
  ecmp-limit       16
```

```
graceful-restart
no as-dot-notation
timers
 holdtime               65535
 advertisement-interval 65535
 graceful-restart-timer 43200
 eor-timer              3600
!
address-family ipv4
 advertise bgp
 advertise ospf external
 advertise connected
 advertise static
 advertise eigrp
 advertise lisp
 advertise isis
!
 address-family ipv6
 advertise bgp
 advertise connected
 advertise static
 advertise eigrp
 advertise lisp
 advertise isis
```

outbound tloc-color

To enable Cisco SD-WAN Controller route filtering by TLOC color, use the **outbound tloc-color** command in filter route configuration mode. To disable route filtering, use the **no** form of the command.

outbound tloc-color

no outbound tloc-color

Command Default

The command is disabled.

Command Modes

filter route configuration (config-filter-route)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	This command was introduced.

Example

```
vsmart# config
Entering configuration mode terminal
vsmart(config)# omp
vsmart(config-omp)# filter-route
vsmart(config-filter-route)# outbound tloc-color
vsmart(config-filter-route)# exit
vsmart(config-omp)# exit
vsmart(config)#
```

The following example shows the same configuration using a CLI template in Cisco SD-WAN Manager:

```
omp
 filter-route
  outbound tloc-color
!
```

overlay-as (omp)

To configure a BGP Autonomous System (AS) number that OMP advertises to the BGP neighbors of a router, use the **overlay-as** command in OMP configuration mode. To remove a BGP AS number that OMP advertises to the BGP neighbors of a router, use the **no** form of this command.

overlay-as *as-number*
no overlay-as

Syntax Description

as-number	Local AS number to advertise to the router's BGP neighbors. You can specify the AS number in 2-byte ASDOT notation (1 through 65535) or in 4-byte ASDOT notation (1.0 through 65535.65535).

Command Default

No AS number is configured.

Command Modes

OMP configuration (config-omp)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

When OMP routes are redistributed into BGP, the confgured AS number is prepended to the BGP AS path.

Examples

The following example shows how to configure OMP on a router:

```
sdwan
 omp
  no shutdown
  overlay-as 4294967295
  send-path-limit 16
  ecmp-limit 16
  graceful-restart
  no as-dot-notation
  timers
   holdtime 65535
   advertisement-interval 65535
   graceful-restart-timer 43200
   eor-timer 3600
  !
  address-family ipv4
   advertise bgp
   advertise ospf external
   advertise connected
```

```
 advertise static
 advertise eigrp
 advertise lisp
 advertise isis
!
address-family ipv6
 advertise bgp
 advertise connected
 advertise static
 advertise eigrp
 advertise lisp
 advertise isis
```

send-path-limit (omp)

To configure the maximum number of equal-cost routes that are advertised per prefix, use the **send-path-limit** command in OMP configuration mode. To remove the maximum number of equal-cost routes that are advertised per prefix, use the **no** form of this command.

send-path-limit *number-of-routes*
no send-path-limit *number-of-routes*

Syntax Description

number-of-routes	Maximum number of equal-cost routes that a router advertises to a Cisco SD-WAN Controller or that a Cisco SD-WAN Controller redistributes to routers. A route is a route–TLOC tuple. Each TLOC consists of an IP address, color, and encap. Beginning with Cisco Catalyst SD-WAN Control Components Release 20.8.x, for a Cisco SD-WAN Controller operating within a Hierarchical SD-WAN architecture, the controller can provide up to 32 routes to edge devices. When an edge device installs the routes, it uses the OMP algorithm to select the best 16 routes, and forwards traffic on those routes. Range: 1 to 32 routes. In releases earlier than Cisco Catalyst SD-WAN Control Components Release 20.9.x, the range was 1 to 16.

Command Default

4 routes are advertised.

Command Modes

OMP configuration (config-omp)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.
Cisco SD-WAN Controller, Cisco Catalyst SD-WAN Control Components Release 20.8.x	Increased the route limit to 32 when used for a Cisco SD-WAN Controller operating within a Hierarchical SD-WAN architecture.

Examples

The following example shows how to configure OMP on a router:

```
sdwan
 omp
```

```
no shutdown
overlay-as 4294967295
send-path-limit 16
ecmp-limit 16
graceful-restart
no as-dot-notation
timers
 holdtime 65535
 advertisement-interval 65535
 graceful-restart-timer 43200
 eor-timer 3600
!
address-family ipv4
 advertise bgp
 advertise ospf external
 advertise connected
 advertise static
 advertise eigrp
 advertise lisp
 advertise isis
!
address-family ipv6
 advertise bgp
 advertise connected
 advertise static
 advertise eigrp
 advertise lisp
 advertise isis
```

timers

To configure OMP timers on Cisco IOS XE Catalyst SD-WAN devices and Cisco Catalyst SD-WAN Controllers, use **timers** command. When you change an OMP timer on a device, the BFD sessions on that device go down and then come back up. To disable timers, use the **no** form of this command.

timers [**advertisement-interval** *interval* | **eor-timer** *eor-timer* | **graceful-restart-timer** *restart-timer* | **holdtime** *holdtime*]
no timers

Syntax Description

eor-timer *seconds*	End-of-RIB Timer: Specifies how long to wait after an OMP session has gone down and then come back up to send an end-of-RIB (EOR) marker. After this marker is sent, any routes that weren't refreshed after the OMP session came back up are considered to be stale and are deleted from the route table. Range: 1–3600 seconds (1 hour) Default: 300 seconds (5 minutes)

graceful-restart-timer *seconds*	Graceful Restart Timer: Specifies how often the OMP information cache is flushed and refreshed. To disable OMP graceful restart, use the **no omp graceful-restart** command. **Note** The **graceful-restart-timer** is peer driven. That is, WAN edge waits for the timer configured on Cisco vSmart to expire before removing the stale routes from the OMP table and Cisco vSmart waits for the timer configured on WAN Edge. Range: 1–604800 seconds (168 hours, or 7 days) Default: 43200 seconds (12 hours)
holdtime *seconds*	Holdtime Interval: Specifies how long to wait before closing the OMP connection to a peer. If the peer doesn't receive three consecutive keepalive messages within the specified hold time, the OMP connection to the peer is closed. (Note that the keepalive timer is one-third the hold time and isn't configurable.) If the local device and the peer have different hold time intervals, the higher value is used. If you set the hold time to 0, the keepalive and hold timers on the local device and the peer are set to 0. The hold time must be at least two times the hello tolerance interval set on the WAN tunnel interface in VPN 0. To configure the hello tolerance interval, use the hello-tolerance command. Range: 0–65535 seconds Defaults, by Cisco Catalyst SD-WAN Control Components release: • 20.18.x and later: 300 seconds • 20.16.x: 5400 seconds • 20.12.1 to 20.15.x: 300 seconds • Before 20.12.1: 60 seconds Defaults, by Cisco IOS XE Catalyst SD-WAN release: • 17.18.1 and later: 300 seconds • 17.16.x: 5400 seconds
advertisement-interval *seconds*	Update Advertisement Interval: Configures the amount of time between OMP Update packets. Range: 0–65535 seconds Default: 1 second

Command Default

Command Modes OMP configuration mode

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

The following commands configure OMP timers on a Cisco IOS XE Catalyst SD-WAN device.

```
sdwan
omp
no shutdown
graceful-restart
no as-dot-notation
timers
holdtime 65535
advertisement-interval 65535
graceful-restart-timer 43200
eor-timer 3600
exit
!
```

tloc-color-compatibility

To override the default compatibilities of TLOC colors, use the **tloc-color-compatibility** command in system configuration mode. To cancel the configuration, use the **no** form of the command.

tloc-color-compatibility { **compatible** *first-color second-color* | **incompatible** *first-color second-color* }
no tloc-color-compatibility { **compatible** *first-color second-color* | **incompatible** *first-color second-color* }

Syntax Description

compatible *first-color second-color*	Configure two TLOC colors to be compatible, even if they are incompatible by default.
incompatible *first-color second-color*	Configure two TLOC colors to be incompatible, even if they are compatible by default.

Command Default

The command has no default.

Command Modes

system configuration (config-system)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	This command was introduced.

Usage Guidelines

Using route filtering, Cisco SD-WAN Controllers can reduce the number of routes that they advertise to routers in the network, to exclude routes that are not relevant to a particular device. The filtering is based on the colors of TLOCs on each device: For each individual device, the Cisco SD-WAN Controller does not advertise routes that are not compatible with any of the device's TLOCs. For example, if a router only has a

TLOC with color mpls, which is a private color, then a Cisco SD-WAN Controller does not advertise a route for a TLOC of with the public-internet color, because the router cannot resolve this public route.

Example

This example, executed on a Cisco SD-WAN Controller, does the following:

- Configures the lte and private1 TLOC colors to be compatible
- Configures the private1 and private2 TLOC colors to be compatible
- Configures the lte and default TLOC colors to be incompatible
- Configures the lte and 3g TLOC colors to be incompatible

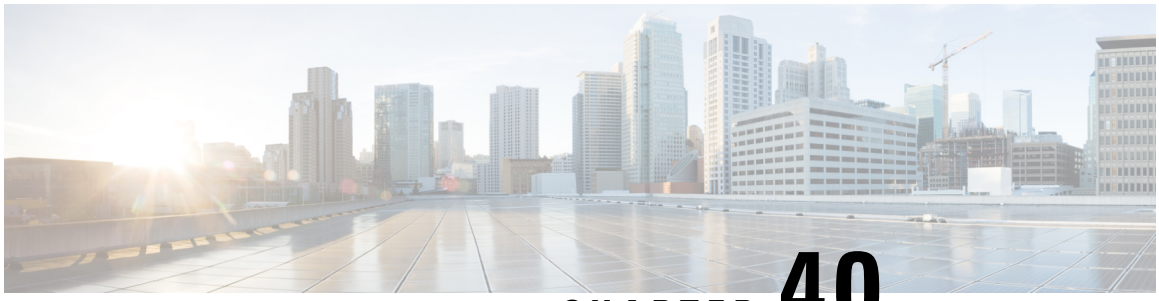
```
vsmart(config)# system
vsmart(config-system)# host-name vm1
vsmart(config-system)# tloc-color-compatibility
vsmart(config-tloc-color-compatibility)# compatible lte private1
vsmart(config-compatible-lte/private1)# exit
vsmart(config-tloc-color-compatibility)# compatible private1 private2
vsmart(config-compatible-private1/private2)# exit
vsmart(config-tloc-color-compatibility)# incompatible lte default
vsmart(config-incompatible-lte/default)# exit
vsmart(config-tloc-color-compatibility)# incompatible lte 3g
vsmart(config-incompatible-lte/3g)# exit
vsmart(config-tloc-color-compatibility)# exit
vsmart(config-system)# exit
vsmart(config)#
```

The following example shows the same configuration using a CLI template in Cisco SD-WAN Manager:

```
system
 host-name vm1
 tloc-color-compatibility
  compatible lte private1
  !
  compatible private1 private2
  !
  incompatible lte default
  !
  incompatible lte 3g
  !
 !
```

To reverse a **compatible** or **incompatible** command, use the **no** form, as follows:

```
vsmart(config-tloc-color-compatibility)# no compatible lte private1
```



CHAPTER 40

OSPF Commands

- area nssa, on page 541
- area range, on page 542
- auto-cost, on page 543
- compatible rfc1583, on page 543
- default-information originate (OSPF), on page 544
- distance ospf, on page 545
- max-metric router-lsa-ospf, on page 546
- router-id, on page 547
- router ospf, on page 547
- timers throttle spf, on page 548

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 *area-id* **nssa** [**no-summary**]
no area *area-id* **nssa** [**no-summary**]

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-summary	(Optional) Allows an area to be an NSSA but not have summary routes injected into it.

Command Default

No NSSA area is defined.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE area nssa command.

Examples

The following example makes area 1 an NSSA area:

```
router ospf 1
 area 4294967295 nssa no-summary
```

area range

To consolidate and summarize routes at an area boundary, use the **area range** command in router configuration mode. To disable this function, use the **no**form of this command.

area *area-id* **range** *ip-address/mask* [**advertise** | **cost** *cost* | **not-advertise**]
no area *area-id* **range** *ip-address/mask* [**advertise** | **cost** *cost* | **not-advertise**]

Syntax Description

area-id	Identifier of the area about which routes are to be summarized. It can be specified as either a decimal value or as an IPv6 prefix.
ip-address/mask	IPv4 prefix and prefix length.
advertise	(Optional) Sets the address range status to advertise and generates a Type 3 summary link-state advertisement (LSA).
not-advertise	(Optional) Sets the address range status to DoNotAdvertise. The Type 3 summary LSA is suppressed, and the component networks remain hidden from other networks.
cost *cost*	(Optional) Metric or cost for this summary route, which is used during OSPF SPF calculation to determine the shortest paths to the destination. The value can be 0 to 16777215.

Command Default

This command is disabled by default.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE area range command.

Examples

The following is an example of this command

```
router ospf 10
  area 4294967295 range 10.1.1.0 255.255.255.0 not-advertise
  area 4294967295 range 192.168.1.0 255.255.255.0 cost 16777214
  area 4294967295 range 172.16.5.0 255.255.255.0 advertise
```

auto-cost

To control how Open Shortest Path First (OSPF) calculates default metrics for the interface, use the **auto-cost**command in router configuration mode. To assign cost based only on the interface type, use the **no** form of this command.

auto-cost reference-bandwidth *mbps*
no auto-cost reference-bandwidth

Syntax Description

reference-bandwidth *mbps*	Rate in Mbps (bandwidth). The range is from 1 to 4294967; the default is 100.

Command Default

100 Mbps

Command Modes

Router configuration (config-router)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE auto-cost command.

Examples

The following example changes the cost of the FDDI link to 10, while the gigabit Ethernet link remains at a cost of 10. Thus, the link costs are differentiated.

```
router ospf 10
 auto-cost reference-bandwidth 100
```

compatible rfc1583

To restore the method used to calculate summary route costs per RFC 1583, use the **compatible rfc1583** in router configuration mode. To disable RFC1583 compatibility, use the **no** form of this command.

compatible rfc1583
no compatible rfc1583

Syntax Description

This command has no arguments or keywords.

Command Default

Compatible with RFC 1583.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE compatible rfc1583 command.

Examples

The following example shows how to disable the default RFC 1583 optimization for OSPFv2:

```
Device(config-router)# no compatible rfc1583
```

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* }
no default-information originate { **always** **metric** *metric-value* | **metric-type** *type-value* }

Syntax Description

always	(Optional) Always advertises the default route regardless of whether the software has a default route. **Note** The **always** keyword includes the following exception when the route map is used. When a route map is used, the origination of the default route by OSPF is not bound to the existence of a default route in the routing table and the **always** keyword is ignored.
metric *metric-value*	(Optional) Metric used for generating the default route. If you omit a value and do not specify a value using the **default-metric** router configuration command, the default metric value is 10. The value used is specific to the protocol.
metric-type *type-value*	(Optional) External link type associated with the default route that is advertised into the OSPF routing domain. It can be one of the following values: • Type 1 external route. • Type 2 external route. The default is type 2 external route.

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)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE default-information originate command.

Examples

The following example specifies a metric for the default route that is redistributed into the OSPF routing domain and specifies an external metric type of 1:

```
router ospf 10
 default-information originate metric-type 1
```

distance ospf

To define Open Shortest Path First (OSPF) route administrative distances based on route type, use the **distance ospf** command in router address family topology or router configuration mode. To restore the default value, use the **no** form of this command.

distance ospf { **external** *dist1* | **inter-area** *dist2* | **intra-area** *dist3* }
no distance ospf

Syntax Description

external *dist1*	(Optional) Sets the distance for routes from other routing domains, learned by redistribution. Range is 1 to 255. The default value is 110.
inter-area *dist2*	(Optional) Sets the distance for all routes from one area to another area. Range is 1 to 255. The default value is 110.
intra-area *dist3*	(Optional) Sets the distance for all routes within an area. Range is 1 to 255. The default value is 110.

Command Default

dist1 : 110

dist2 : 110

dist3 : 110

Command Modes

Router configuration (config-router)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE distance ospf command.

Router A Configuration

```
router ospf 1
 distance ospf external 110
  distance ospf inter-area 110
  distance ospf intra-area 110
```

max-metric router-lsa-ospf

To configure the Open Shortest Path First (OSPF) protocol to advertise a maximum metric so that other routers do not prefer the router as an intermediate hop in their shortest path first (SPF) calculations, use the **max-metric router-lsa** command. To disable the advertisement of a maximum metric, use the **no** form of this command.

max-metric router-lsa [**on-startup** *seconds*]

no max-metric router-lsa [**on-startup** *seconds*]

Syntax Description

on-startup	(Optional) Configures the router to advertise a maximum metric at startup.
seconds	(Optional) Maximum metric (in seconds) that is advertised for the specified time interval. The configurable range is from 5 to 86400 seconds. The default is 600 seconds.

Command Default

Originates router link-state advertisements (LSAs) with normal link metrics.

Command Modes

Router configuration mode (config-router)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

Use the max-metric router-lsa command to originate LSAs with a maximum metric (LSInfinity: 0xFFFF) through all nonstub links. This command allows Border Gateway Protocol (BGP) routing tables to converge without attracting transit traffic (if there are not alternate lower cost paths to the router). The router advertises accurate (normal) metrics after the configured or default timers expire or after BGP sends a notification that routing tables have converged.

Note Directly connected links in a stub network are not affected by the configuration of a maximum or infinite metric because the cost of a stub link is always set to the output interface cost.

You can use the max-metric router-lsa command in the following situations:

- Reloading a router. After a router is reloaded, Interior Gateway Protocols (IGPs) converge very quickly, and other routers may try to forward traffic through the newly reloaded router. If the router is still building BGP routing tables, the packets that are destined for other networks that the router has not learned through BGP may be dropped.

- Introducing a router into a network without routing traffic through it. You might want to connect a router to an OSPF network but not want real traffic to flow through the router if there are better alternate paths. If no alternate paths exist, then this router would still accept transit traffic.

This command requires the LAN Base Services license.

Examples

This example shows how to configure a router that is running OSPF to advertise a maximum metric for 100 seconds:

```
Device(config)# router ospf 100
Device(config-router)# max-metric router-lsa on-startup 100
```

router-id

To use a fixed router ID, use the **router-id** command in router configuration mode. To force Open Shortest Path First (OSPF) to use the previous OSPF router ID behavior, use the **no** form of this command.

router-id *ip-address*
no router-id *ip-address*

Syntax Description

ip-address	Router ID in IP address format.

Command Default

No OSPF routing process is defined.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE router-id command.

Examples

The following example specifies a fixed router-id:

```
router-id 10.1.1.1
```

router ospf

To configure an Open Shortest Path First (OSPF) routing process, use the **router ospf** command in global configuration mode. To terminate an OSPF routing process, use the **no**form of this command.

router ospf *process-id*
no router ospf *process-id*

Syntax Description

process-id	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.

Command Default

No OSPF routing process is defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

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 10:

```
Router(config)# router ospf 10
```

timers throttle spf

To turn on Open Shortest Path First (OSPF) shortest path first (SPF) throttling, use the **timers throttle spf** command in the appropriate configuration mode. To turn off OSPF SPF throttling, use the **no** form of this command.

timers throttle spf *spf-start spf-hold spf-max-wait*
no timers throttle spf *spf-start spf-hold spf-max-wait*

Syntax Description

spf-start	Initial delay to schedule an SPF calculation after a change, in milliseconds. Range is from 1 to 600000. In OSPF for IPv6, the default value is 5000.
spf-hold	Minimum hold time between two consecutive SPF calculations, in milliseconds. Range is from 1 to 600000. In OSPF for IPv6, the default value is 10,000.
spf-max-wait	Maximum wait time between two consecutive SPF calculations, in milliseconds. Range is from 1 to 600000. In OSPF for IPv6, the default value is 10,000.

Command Default

SPF throttling is not set.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

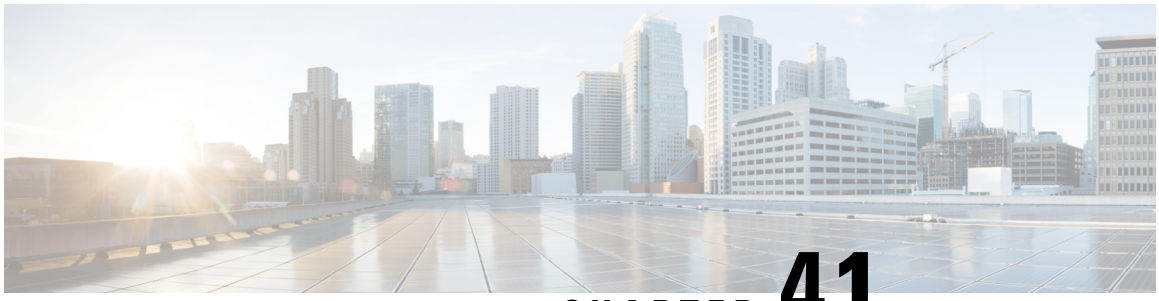
Usage Guidelines

For usage guidelines, see the Cisco IOS XE timers throttle spf command.

Examples

The following example shows how to configure a router with the delay, hold, and maximum interval values for the **timers throttle spf** command:

```
router ospf 1 10
  timers throttle spf 200 1000 10000
```



CHAPTER 41

Policy Commands

- access-list, on page 552
- action (centralized policy), on page 554
- action (localized policy), on page 556
- app-agg-node, on page 558
- apply-policy, on page 559
- app-probe-class, on page 560
- app-route-policy, on page 561
- app-visibility, on page 562
- app-visibility-ipv6, on page 563
- burst, on page 563
- class (class-map), on page 565
- cos, on page 565
- count, on page 566
- data-policy, on page 567
- default-action, on page 567
- destination-ip, on page 568
- exceed, on page 569
- flow-visibility, on page 570
- flow-visibility-ipv6, on page 570
- icmp-echo, on page 571
- implicit-acl-on-bind-intf , on page 572
- inspect, on page 572
- ip-prefix, on page 573
- ip sla, on page 574
- ip sla reaction-configuration, on page 574
- ip sla responder, on page 576
- ip sla schedule, on page 577
- ip visibility cache entries, on page 578
- ipv6 access-list, on page 579
- ipv6 visibility cache entries, on page 579
- jitter, on page 580
- lists, on page 580
- lists data-prefix-list, on page 582

- lists (tag instance), on page 583
- loss, on page 584
- match (access-control-list), on page 585
- match as-path, on page 587
- match (data policy), on page 588
- match ip address, on page 590
- match protocol attribute application-group, on page 591
- parameter-map type inspect, on page 592
- policer, on page 592
- policy, on page 594
- policy ip visibility, on page 595
- policy log-rate-limit, on page 596
- queue-limit, on page 597
- rate, on page 599
- request-data-size, on page 600
- rewrite-rule, on page 600
- service-area, on page 602
- service-policy, on page 603
- set ip vrf, on page 604
- set ip next-hop verify-availability, on page 605
- sequence, on page 606
- sequence (access-control-list), on page 607
- sla-class, on page 608
- sig, on page 609
- site-list, on page 610
- tag (IP SLA), on page 611
- tag-instances, on page 612
- track ip sla, on page 613
- udp-jitter, on page 614
- utd-policy, on page 615
- vpn-list, on page 615
- vrf (IP SLA), on page 616

access-list

To define the access list, use the **access-list** command in policy configuration mode. To remove the access list, use the **no** form of this command.

access-list *access-list-name* [**sequence** *sequence-value* [**match** [**destination-ip** *dest-ip/length* | **source-ip** *src-ip/length* | **destination-port** *dest-port-range* | **source-port** *src-port-range* | **destination-data-prefix-list** *prefix* | **source-data-prefix-list** *prefix* | **destination-tag-instance** *dest-tag-name* | **source-tag-instance** *src-tag-name*] **action** { **accept** | [**class** | **count**] | **drop** | **count** } | **action**] | **default-access** | **drop accept**]

no access-list

Syntax Description

destination-data-prefix-list	(Optional) Specifies the destination prefix list.

destination-ip	(Optional) Specifies the list of destination addresses.
destination-port	(Optional) Specifies the list of destination ports.
count	(Optional) Specifies the number of packets/bytes matching this rule drop.
destination-tag-instance	(Optional) Specifies the name of the destination tag instance. Valid range is from 1 to 127 characters.
source-data-prefix-list	(Optional) Specifies the source data prefix list.
source-ip	(Optional) Specifies the list of source IP addresses.
source-port	(Optional) Specifies the list of source ports.
source-tag-instance	(Optional) Specifies the name of the source tag instance. Valid range is from 1 to 127 characters.

Command Default

The access list defaults to an implicit deny statement for everything. An implicit deny statement terminates an access list.

Command Modes

Policy configuration (config-policy)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This command was modified. Policy match configuration is enhanced to include **source-tag-instance** and **destination-tag-instance** keyword parameters in ACL-matching attributes.

Usage Guidelines

After ACL is defined, it can be applied to an interface.

Examples

The following is a sample output of this command:

```
access-list acl1
   sequence 10
    match
     destination-ip 172.16.5.10
    !
    action drop
   default-action accept
    action drop
     count 192-167-199-DROP-CNT
  access-list 4451-Marking-Spoke
   sequence 1
    match
     destination-ip 172.16.10.5
    !
    action accept
     count SSL
     class LLQ
```

```
     count EXCHANGE
     class CONTROL-SIGNALING
```

The following example shows how to configure **source-tag-instance** in a localized policy:

```
policy
 lists
  data-prefix-list pfx1
   ip-prefix 10.20.24.0/24
  !
 !
 access-list acl
  sequence 10
   match
    source-tag-instance red
   !
   action accept
    count acl_input_wc
   !
  !
  default-action drop
 !
!
```

action (centralized policy)

To define the action to take when the match portion in a match–action pair is met, use the **action** command in sequence configuration mode. To remove configured sub-actions or reset the action to the default of drop, use the **no** form of this command.

action { **drop** { **count** *counter-name* | **log** } | **accept** { **count** *counter-name* | **nat use-vpn** *0* { } | **log** | **local-tloc** | **policer** *policer-name* | **next-hop** *ipv4-address* **next-hop-loose** | **set** { **vpn** *vpn-number* } | { **set tloc** *ip-address* **color** *color* } } }

no action { **drop** { **count** *counter-name* | **log** } | **accept** { **count** *counter-name* | **nat use-vpn** *0* { } | **log** | **local-tloc** | **policer** *policer-name* | **next-hop** *ipv4-address* **next-hop-loose** | **set** { **vpn** *vpn-number* } | { **set tloc** *ip-address* **color** *color* } } }

Syntax Description

drop	Defines the action to drop matching packets.
accept	Defines the action to accept matching packets and to perform any specified actions.
nat use-vpn *0*	Ensures that matching traffic is sent to VPN 0 after the source IP is translated, based on the policy match criteria.
count *counter-name*	Counts the packets that match the match criteria, saving the information to the specified filename.
log	Logs the packet headers into system logging (syslog) files.

set tloc *ip-address* **color** *color* [**encap** *ecapsulation*]	Sets the TLOC identified IP sddress and color Directs matching packets to a TLOC identified by its IP address and color, and optionally, by its encapsulation.*color* can be **3g**, **biz-internet**, **blue**, **bronze**, **custom1**, **custom2**, **custom3**, **default**, **gold**, **green lte**, **metro-ethernet**, **mpls**, **private1** through **private6**, **public-internet**, **red**, and **silver**. By default, *encapsulation* is **ipsec**. It can also be **gre**.
policer *policer-name*	Police the packets using the specified policer.
set dscp *dscp-value*	For QoS, set or overwrite the DSCP value in the packet. Range: 0 through 63.
set local-vpn *local-vpn-number*	Sets the local VPN number. Range: 0 through 65530.
set next-hop *ipv4-address*	Sets the next-hop address. The address must be an IPv4 address.
set next-hop-loose	Routes the traffiic using an available route if the next-hop address is not available. This parameter is supported only for centralized data policies.

Command Default

The default behavior is dropped.

Command Modes

Policy configuration (config-policy)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	Command qualified for use in CLI templates.
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	This command was modified. Added next-hop-loose keyword to redirect application traffic to an available route when next-hop address is not available.
Cisco IOS XE Catalyst SD-WAN Release 17.13.1a	This command was modified. Added the **nat use vpn***0* keyword for NAT66 to configure the centralized data policy.

Usage Guidelines

The sequence numbering feature applies sequence numbers to match-action pairs. The match–action pairs are evaluated in order, by sequence number, starting with the lowest numbered pair and ending when it matches the conditions in one of the pairs.

When a packet matches one of the match conditions, the defined action is taken. Or if no match occurs, the default action is taken.

This command can be used to define the action to take when the match portion in a match–action pair is met.

Note The **set next-hop-loose** option can be applied only if **set next-hop** action is defined.

Example

The following example shows how to create a centralized control policy that changes the TLOC for accepted packets:

```
Device(config)# policy
  control-policy change-tloc
    sequence 10
      action accept
        set tloc 10.1.1.2
```

The following example shows how to create a data policy using next-hop-loose command inorder to route the packet using routing entry from routing table if next-hop is not reachable.

```
show policy from-vsmart
from-vsmart data-policy data_pol_nh1
 direction all
 vpn-list vpn1
  sequence 12
   match
    source-ip 10.20.24.150/32
   action accept
    count data_pol_nh1_ctr
    set
     next-hop 96.0.1.100
     next-hop-loose
  sequence 122
   match
    source-ip 10.20.25.150/32
   action accept
  default-action drop
```

The following example shows how to configure a NAT66 DIA route using a centralized data policy so that data traffic is NATed before entering the overlay tunnel that is located in the transport VPN:

```
Device(config)# policy
 data-policy policy-name
  vpn-list vpn_list
  sequence number
  match
   source-ipv6 ipv6-address
  !
  action accept
   nat use-vpn 0
   nat fallback
   set
    local-tloc-color lte
```

For more information about, see the section *NAT66 DIA With Centralized Data Policy* in *Information About NAT DIA*

action (localized policy)

To define the action to take when the match portion in a match–action pair is met, use the **action** command in access control list sequence configuration mode. To remove configured sub-actions or reset the action to the default of drop, use the **no** form of this command.

action { **drop** { **count** *counter-name* | **log** } | **accept** { **class** *class-name* | **count** *counter-name* | **log** | **mirror** *mirror-name* | **policer** *policer-name* } | **set** { **dscp** *dscp-value* | **local-vpn** *local-vpn-number* | **next-hop** *ipv4-address* **next-hop-loose** } }
no action { **drop** { **count** *counter-name* | **log** } | **accept** { **class** *class-name* | **count** *counter-name* | **log** | **mirror** *mirror-name* | **policer** *policer-name* } | **set** { **dscp** *dscp-value* | **local-vpn** *local-vpn-number* | **next-hop** *ipv4-address* } }

Syntax Description

drop	Defines the action to drop matching packets.
accept	Defines the action to accept matching packets and to perform any specified actions.
count *counter-name*	Counts the packets that match the match criteria, saving the information to the specified filename.
log	Logs the packet headers into system logging (syslog) files.
class *class-name*	Assigns the packets to the specified QoS class name.
mirror *mirror-name*	Mirrors the packets to the specified mirror.
policer *policer-name*	Police the packets using the specified policer.
set dscp *dscp-value*	For QoS, set or overwrite the DSCP value in the packet. Range: 0 through 63.
set local-vpn *local-vpn-number*	Sets the local VPN number. Range: 0 through 65530.

Command Default

The default behavior is dropped.

Command Modes

Access control list sequence configuration (config-sequence-{sequence-number})

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Access control lists (ACLs) perform packet filtering to control which packets move through an interface of a router. The packet filtering provides security by helping to limit the network traffic, restrict the access of users and devices to a network, and prevent the traffic from leaving a network interface. An access control list is a sequential list consisting of match-action pairs.

The sequence numbering feature applies sequence numbers to match-action pairs. The match–action pairs are evaluated in order, by sequence number, starting with the lowest numbered pair and ending when it matches the conditions in one of the pairs.

When a packet matches one of the match conditions, the defined action is taken. Or if no match occurs, the default action is taken.

This command can be used to define the action to take when the match portion in a match–action pair is met.

Example

The following example creates an access control list named ACL-TEST-1, defines sequence #10, enters the match configuration mode, specifies destination IP 10.10.10.10/32 as a match parameter, and defines the action to drop and logs the packet when matched.

```
Device(config)# policy
Device(config-policy)# access-list ACL-TEST-1
Device(config-access-list-ACL-TEST-1)# sequence 10
Device(config-sequence-10)# match
Device(config-match)# destination-ip 10.10.10.10/32
Device(config-match)# exit
Device(config-sequence-10)# action drop
Device(config-action)# log
```

The following example creates an access control list named ACL-TEST-1, defines sequence #20, enters the match configuration mode, specifies packet length of 10 as a match parameter and defines the action to accept and applies the policer policy POL1 when matched.

```
Device(config)# policy
Device(config-policy)# access-list ACL-TEST-1
Device(config-access-list-ACL-TEST-1)# sequence 20
Device(config-sequence-20)# match
Device(config-match)# packet-length 10
Device(config-match)# exit
Device(config-sequence-20)# action accept
Device(config-action)# policer POL1
```

Table 33: Related Commands

Commands	Description
match	Enters the match configuration mode or to define match parameters.

app-agg-node

To set the maximum rate of Flexible NetFlow (FNF) records of aggregated traffic data that a device sends to Cisco SD-WAN Manager, use the **app-agg-node** command in policy configuration mode on a device. To restore the default limit, use the **no** form of the command.

app-agg-node *max-records-per-minute*

no app-agg-node

Syntax Description

max-records-per-minute	Maximum number of FNF records per minute of aggregated traffic data for a device to send to Cisco SD-WAN Manager. Range: 16 to 10000 FNF records per minute Default: 10000 FNF records per minute

Command Modes

Policy configuration (config-policy)

Command Default

10000 FNF records per minute

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.14.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

When traffic flow visibility is enabled (see Configure Global Flow Visibility), devices in the network send raw and aggregated traffic flow data to Cisco SD-WAN Manager.

To aggregate flow data, routers use 4-tuples of flow data (containing VPN ID, application name, ingress interface of the flow, and egress interface of the flow) as a key for consolidating the raw data of multiple flows. The router consolidates each flow for which the 4-tuple is identical into a single aggregated FNF record.

Cisco SD-WAN Manager uses the aggregated data to provide a high-level view of network traffic flow information. The aggregated data shows the network applications that are producing traffic, but is less granular than the full traffic flow data. It does not provide source and destination addresses, or source and destination ports for traffic flows.

You can configure a maximum rate of aggregated traffic data FNF records that a device can send to reduce the performance demands (CPU and memory) on the device. This may be helpful when there is a large number of applications producing network traffic.

Example 1

The following configures a device to send a maximum of 1000 FNF records per minute.

```
Device(config)# policy
Device(config-policy)# app-agg-node 1000
```

Example 2

The following restores a device to the default value of sending a maximum of 10000 FNF records per minute.

```
Device(config)# policy
Device(config-policy)# no app-agg-node
```

apply-policy

To have a policy take effect by applying it to sites within the overlay network (on Cisco vSmart Controllers only), use the **apply-policy** command in the policy lists configuration mode. To remove the listing of sites, use the **no apply-policy** form of this command.

apply-policy

no apply-policy

Syntax Description

This command has no arguments or keywords.

Command Default None

Command Modes policy lists configuration (config-lists)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

```
vSmart(config)# apply-policy
vSmart(config-apply-policy)# site-list cedge_1
vSmart(config-site-list-cedge_1)# data-policy sig_ha_zscaler_data_policy_cedge from-service
```

```
vSmart(config)# apply-policy
vSmart(config-apply-policy)# site-list cedge_1
vSmart(config-site-list-cedge_1)# data-policy sig_ha_zscaler_data_policy_cedge from-tunnel
```

```
vSmart(config)# apply-policy
vSmart(config-apply-policy)# site-list cedge_1
vSmart(config-site-list-cedge_1)# data-policy sig_ha_zscaler_data_policy_cedge all
```

app-probe-class

To define a forwarding class and DSCP marking per color that a particular class of applications is forwarded to, use the **app-probe-class** command in global configuration mode.

app-probe-class *app-probe-class-name*

no app-probe-class *app-probe-class-name*

Syntax Description

app-probe-class	Specifies the app-probe-class of SLA class applications that is forwarded to devices.
app-probe-class-name	Specifies the app-probe-class name.

Command Default There are no default values.

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

In the following example, you can create real-time-video app-probe-class with DSCP measurements:

```
vSmart(config)# app-probe-class real-time-video
vSmart(config)# forwarding-class videofc
vSmart(config)# color mpls dscp 34
vSmart(config)# color biz-internet dscp 40
```

```
vSmart(config)# color lte dscp 0
```

app-route-policy

To configure application route policy for the Cisco IOS XE Catalyst SD-WAN devices, use the **app-route-policy** command in the policy configuration mode.

app-route-policy *policy-name*

Syntax Description

app-route-policy *policy-name*	Name of the application-aware routing policy to configure or to apply to a list of sites in the overlay network. *policy-name* can be up to 32 characters long.

Command Modes

Policy configuration (config-policy)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in CLI templates.

Usage Guidelines

For more information about this command, see Policies Configuration guide.

The following example shows how to configure and apply a data policy for application-aware routing:

```
vSmart# show running-config policy
policy
 sla-class test_sla_class
  latency 50
 !
 app-route-policy test_app_route_policy
  vpn-list vpn_1_list
   sequence 1
    match
     protocol 6
    !
    action sla-class test_sla_class strict
   !
   sequence 2
    match
     protocol 17
    !
    action sla-class test_sla_class
   !
   sequence 3
    match
     protocol 1
    !
    action sla-class test_sla_class strict
   !
  !
 !
 lists
  vpn-list vpn_1_list
   vpn 1
  !
```

```
  site-list site_500
   site-id 500
  !
  site-list site_600
   site-id 600
  !
 !
!
apply-policy
 site-list site_500
  app-route-policy test_app_route_policy
 !
!
```

The following example shows how to configure a policy for application-aware routing:

```
policy
  app-route-policy policy-name
    vpn-list list-name
      default-action sla-class sla-class-name
      sequence number
        match
          app-list list-name
          destination-data-prefix-list list-name
          destination-ip prefix/length
          destination-port number
          dns (request | response)
          dns-app-list list-name
          dscp number
          plp (high | low)
          protocol number
          source-data-prefix-list list-name
          source-ip prefix/length
          source-port address
        action
          backup-sla-preferred-color colors
          count counter-name
          log
          sla-class sla-class-name [strict] [preferred-color colors]
```

app-visibility

To enable application visibility so that a router can monitor and track the applications running on the LAN use the **app-visibility** command. Use the **no** form of this command to disable application visibility.

app-visibility

Command Default

Disabled.

Command Modes

Policy configuration (config-policy)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines To enable NBAR feature to recognize applications. Use the **show sdwan app-fwd dpi** command to see DPI flows.

Examples Enable application-visibility on a router:

```
Router(config)# policy
Router(config-policy)# app-visibility
```

app-visibility-ipv6

To enable application visibility IPv6, so that a router can monitor and track the applications running on the LAN use the **app-visibility-ipv6** command. Use the **no** form of this command to disable application visibility IPv6.

app-visibility-ipv6

Command Default Disabled.

Command Modes Policy configuration (config-policy)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines To enable NBAR feature to recognize applications. Use the **show sdwan app-fwd dpi** command to see DPI flows.

Examples Enable application-visibility on a router:

```
Router(config)# policy
Router(config-policy)# app-visibility-ipv6
```

burst

To define the burst size for a policer profile, use the **burst** command in policer configuration mode.

burst *burst-size*

Note Burst is a required parameter in a policer profile. Entering **no burst** *burst-size* is valid, but causes **commit** to fail.

Syntax Description

burst-size	Maximum traffic burst size, in bytes. The range is from 15000 to 10000000.

Command Default None

Command Modes Policer configuration (config-policer-{profile-name})

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines To configure policing parameters, create a policer that specifies the maximum bandwidth and burst rate for traffic on an interface, and how to handle traffic that exceeds these values.

This command can be used to define the burst size for a policer profile.

Example

The following example defines a policer profile named pol1. It sets the rate to 500,000,000 bps, and burst size to 15,000 bytes, and configures to drop the traffic if the burst size or traffic rate is exceeded.

```
Device(config)# policy
Device(config-policy)# policer pol1
Device(config-policy-pol1)# rate 500000000
Device(config-policy-pol1)# burst 15000
Device(config-policy-pol1)# exceed drop
```

The following example applies a policer using an Access List named ACL-TEST-1.

```
Device(config)# policy
Device(config-policy)# access-list ACL-TEST-1
Device(config-access-list-ACL-TEST-1)# sequence 1
Device(config-sequence-1)# action drop
Device(config-action)# policer pol1
```



Note Rate, burst, and exceed must be defined before committing, otherwise the commit is aborted.

Table 34: Related Commands

Commands	Description
exceed	Action to take when the burst size or traffic rate is exceeded.
rate	Bandwidth for 1G interfaces, the range is from 8 to 1000000000 bps; for 10G interfaces, the range is from 8 to 10000000000 bps.

class (class-map)

To specify the name of the class whose policy you want to create or change before you configure its policy, use the **class**command in class-map configuration mode. To remove a class from the class map, use the **no** form of this command.

class *class-name*
no class { *class-name* }

Syntax Description

class-name	Name of the class to be configured or whose policy is to be modified. The class name is used for both the class map and to configure a policy for the class in the policy map.

Command Default

No class is specified.

Command Modes

Class-map configuration (config-class-map)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE, class command.

Examples

The following is an example of this command:

```
Device(config)# policy
Device(config-policy)# class-map
Device(config-class-map)# class VOICE queue 0
```

cos

To set the class of service (CoS) for a Cisco IOS IP Service Level Agreements (SLAs) Ethernet operation, use the **cos** command in the appropriate submode of IP SLA configuration or IP SLA Ethernet monitor configuration mode. To return to the default value, use the **no** form of this command.

cos-value	Class of service (CoS) value. The range is from 0 to 7. The default is 0.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE cos command.

Examples

The following example shows how to configure this command:

```
Interface interface-name
 cfm mep domain domain-name mpid id service service-name
  alarm notification all*
  cos 0-7
```

count

To specify the number of packets that matches the match criteria, use the **count** command in the action configuration mode. To remove the count that matches the match criteria, use the **no** form of this command.

count { *counter-name* }

no count { *counter-name* }

Syntax Description

counter-name	Specifies the count of the packets that match the match criteria, and saving the information to a specified filename.

Command Default

None

Command Modes

action configuration (config-action)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For more information about this command, see Centralized Policy.

The following example creates an access control list named ACL-TEST-1, defines sequence #10, enters the match configuration mode, specifies destination IP 10.10.10.10/32 as a match parameter, defines the action to accept, and specifies the packets that match the match criteria in the seqcnt_100 file.

```
Device(config)# policy
Device(config-policy)# access-list ACL-TEST-1
Device(config-access-list-ACL-TEST-1)# sequence 10
Device(config-sequence-10)# match
Device(config-match)# destination-ip 10.0.0.0/8
Device(config-match)# exit
Device(config-sequence-10)# action accept
Device(config-action)# count seqcnt_100
```

data-policy

To configure or apply a centralized data policy based on data packet header fields (on Cisco vSmart controllers only), use the **data-policy** command in policy configuration mode. To remove the configured centralized data policy for deep packet inspection, use the **no** form of this command.

data-policy { *policy-name* }

no data-policy { *policy-name* }

Syntax Description

policy-name	Specifies the name of the centralized data policy to configure or to apply to a list of sites in the overlay network. The maximum characters allowed are 32.

Command Default

None

Command Modes

Policy configuration (config-policy)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For more information about this command, see configuring the deep packet inspection in the Policies Configuration Guide.

```
vSmart(config)# policy
vSmart(config-policy)# data-policy sig_ha_zscaler_data_policy_cedge
```

default-action

To configure the default action to be taken when the match condition in an access list isn't met for the Cisco IOS XE Catalyst SD-WAN devices, use the **default-action** command in the policy access list configuration mode. To remove the default configuration, use the **no default-action** form of this command.

default-action [**drop**] { **accept** | **drop** }

no default-action

Syntax Description

accept|**drop**	Specifies the default action to take if a route being evaluated by a policy matches none of the match conditions. If you configure a policy and define an access list with one or more match–action sequences, the default action, is to either accept or drop the item, depending on the policy type.

Command Default

None

Command Modes policy access list configuration (config-access-list)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines For more information about this command, see Localized Policy.

The following example shows that if a packet being evaluated doesn't match any of the match conditions in an access list, a default action is applied to this packet. By default, the packet is dropped.

```
Device(config)# policy
Device(config-policy)# access-list ACL-TEST-1
Device(config-access-list-ACL-TEST-1)# sequence 10
Device(config-sequence-10)# match
Device(config-match)# destination-ip 10.10.10.10/32
Device(config-match)# exit
Device(config-match)# exit
Device(config-access-list-ACL-TEST-1)# default-action accept
```

destination-ip

To list the destination addresses for an access control list, use the **destination-ip** command in the match configuration mode. To remove the list of destination addresses, use the **no** form of this command.

destination-ip { *ipv4-prefix/prefix-length* }

no destination-ip { *ipv4-prefix/prefix-length* }

Syntax Description

ipv4-prefix/prefix-length	Specifies IPv4 prefix in dotted decimal and the length of the IPv4 prefix. Specifies the prefix-length, which is a decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.

Command Default None

Command Modes match configuration (config-match)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines For more information about this command, see Centralized Policy.

```
Device(config)# policy
Device(config-policy)# access-list ACL-TEST-1
Device(config-access-list-ACL-TEST-1)# sequence 10
Device(config-sequence-10)# match
```

```
Device(config-match)# destination-ip 10.10.10.10/32
Device(config-match)# exit
```

exceed

To define the exceed action for a policer profile, use the **exceed** command in policer configuration mode.

exceed { *drop* | *remark* }

Syntax Description

drop	Drops excess traffic when the burst size or traffic rate is exceeded. The drop action is equivalent to setting the packet loss priority (PLP) to low.
remark	Remarks the traffic. The remark action sets the PLP to high.

Command Default

None

Command Modes

Policer configuration (config-policer-{profile-name})

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

To configure policing parameters, create a policer that specifies the maximum bandwidth and burst rate for traffic on an interface, and how to handle traffic that exceeds these values.

This command can be used to define the action to take if the burst size or traffic rate is exceeded.

Example

The following example defines a policer profile named pol1. It sets the rate to 500,000,000 bps, and burst size to 15,000 bytes, and configures to drop the traffic if the burst size or traffic rate is exceeded.

```
Device(config)# policy
Device(config-policy)# policer pol1
Device(config-policy-pol1)# rate 500000000
Device(config-policy-pol1)# burst 15000
Device(config-policy-pol1)# exceed drop
```

The following example applies a policer using an Access List named ACL-TEST-1.

```
Device(config)# policy
Device(config-policy)# access-list ACL-TEST-1
Device(config-access-list-ACL-TEST-1)# sequence 1
Device(config-sequence-1)# action drop
Device(config-action)# policer pol1
```

Note Rate, burst, and exceed must be defined before committing, otherwise the commit is aborted.

Table 35: Related Commands

Commands	Description
burst	Maximum traffic burst size, in bytes.The range is from 15000 to 10000000.
rate	Bandwidth for 1G interfaces, the range is from 8 to 1000000000 bps; for 10G interfaces, the range is from 8 to 10000000000 bps.

flow-visibility

To enable flow visibility so that a router can perform traffic flow monitoring on traffic coming to the router from the LAN use the **flow-visibility** command. To disable the flow visibility use the **no** form of this command.

flow-visibility

no flow-visibility

Command Default

Disabled.

Command Modes

Policy configuration (config-policy)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

Use the **show sdwan app-fwd cflowd** command to enable cflowd flow monitoring.

Examples

The following is an example of this command

```
Router(config)# policy
Router(config-policy)# flow-visibility
```

flow-visibility-ipv6

To enable flow visibility IPv6, so that a router can perform traffic flow monitoring on traffic coming to the router from the LAN use the **flow-visibility-ipv6** command. To disable the flow visibility use the **no** form of this command.

flow-visibility-ipv6

no flow-visibility-ipv6

Command Default

Disabled.

Command Modes

Policy configuration (config-policy)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

Use the **show sdwan app-fwd cflowd** command to enable cflowd flow monitoring.

Examples

The following is an example of this command

```
Router(config)# policy
Router(config-policy)# flow-visibility-ipv6
```

icmp-echo

To configure an IP Service Level Agreements (SLAs) Internet Control Message Protocol (ICMP) echo operation, use the **icmp-echo**command in IP SLA configuration mode.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE icmp-echo command

Examples

In the following example, IP SLAs operation 10 is created and configured as an echo operation using the ICMP protocol and the destination IPv4 address 10.16.1.175:

```
Device# config-transaction
Device(config)# ip sla 10
Device(config-ip-sla)# icmp-echo 10.16.1.175
Device(config-ip-sla-echo)#
```

In the following example, IP SLAs operation 11 is created and configured as an echo operation using the ICMP protocol and the destination IPv6 address 2001:DB8:100::1:

```
Device# config-transaction
Device(config)# ip sla 11
Device(config-ip-sla)# icmp-echo 2001:DB8:100::1
Device(config-ip-sla-echo)#
```

implicit-acl-on-bind-intf

To enable implicit ACL protection on a physical interface (bound to a loopback interface), use the **implicit-acl-on-bind-intf**command in the global configuration mode. To remove this change, use the no form of this command.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	Command qualified for use in Cisco vManage CLI templates.

Examples

The following example shows how to enable a physical interface as a TLOC.

```
Device(config)# sdwan interface Loopback1
Device(config-interface-Loopback1)# tunnel-interface
Device(config-tunnel-interface)# encap ipsec
Device(config-tunnel-interface)# color 3g
Device(config-tunnel-interface)# bind GigabitEthernet1
Device(config-tunnel-interface)#implicit-acl-on-bind-intf
```

inspect

To enable Cisco IOS stateful packet inspection, use the **inspect** command in policy-map-class configuration mode. To disable stateful packet inspection, use the **no** form of this command.

inspect
no inspect

Command Default

Cisco IOS stateful packet inspection is disabled.

Command Modes

Policy-map-class configuration (config-pmap-c)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE inspect command.

Examples

The following example specifies inspection parameters and requests the **inspect** action with the specified inspect parameter:

```
policy-map type inspect mypolicy
 class type inspect inspect-traffic
  inspect
```

ip-prefix

To define an IP prefix for a data-prefix-list or prefix-list, use the **ip-prefix** command in data-prefix-list or prefix-list configuration mode. To remove an IP prefix for a data-prefix-list or prefix-list, use the **no** form of this command.

ip-prefix *IP/length* [**ge** *length*] [**le** *length*]
no ip-prefix *IP/length*

Syntax Description

IP/length	IP address and CIDR.
ge	(Optional) (Prefix-list only, not available for data-prefix-list) Specifies the minimum prefix length to be matched.
le	(Optional) (Prefix-list only, not available for data-prefix-list) Specifies the maximum prefix length to be matched.
length	Specifies the prefix length, ranges from 1 to 32.

Command Default

None

Command Modes

data-prefix-list configuration (config-data-prefix-list-{data-prefix-list list-name})

prefix-list configuration (config-prefix-list-{prefix-list list-name})

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Lists are used to create groupings of similar objects, such as IP prefixes, sites, TLOC addresses, and AS paths, for use when configuring policy match conditions or action operations and for when applying a policy.

Data-prefix-list is a list of prefixes used in data-policy to define prefix and upper layer ports, either individually or jointly, for traffic matching.

Prefix-list is a list of prefixes used in route-maps. This command can be used to define the ip prefix for a data-prefix-list or prefix-list.

Example

The following example defines a data prefix list named Email-Server. The IP prefix of 10.10.10.10/32 is added to the data prefix list Email-Server.

```
Device(config)# policy
Device(config-policy)# lists
Device(config-lists)# data-prefix-list Email-Server
Device(config-data-prefix-list-Email-Server)# ip-prefix 10.10.10.10/32
```

The following example defines a prefix list named Web-Server. The IP prefix of 10.10.0.0/16 is added to the data prefix list Web-Server.

```
Device(config)# policy
Device(config-policy)# lists
Device(config-lists)# prefix-list Web-Server
Device(config-prefix-list-Web-Server))# ip-prefix 10.10.0.0/1
```

ip sla

To begin configuring a Cisco IOS IP Service Level Agreements (SLAs) operation and enter IP SLA configuration mode, use the **ip sla**command in global configuration mode. To remove all configuration information for an operation, including the schedule of the operation, reaction configuration, and reaction triggers, use the **no** form of this command.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE ip sla command.

Configure **static ip sla {value}** before configuring an endpoint-tracker. If you configure endpoint-tracker, which dynamically assigns IP SLA index. When you try to configure SLA through CLI template, if the index is same, then you might get an error stating SLA is already configured.

Examples

The following example shows how to configure a Cisco IOS IP SLA operation.

```
Device# config-transaction
Device(config)# ip sla 1
Device(config-ip-sla)#
```

ip sla reaction-configuration

To configure proactive threshold monitoring parameters for an IP Service Level Agreements (SLAs) operation, use the **ip sla reaction-configuration** command in global configuration mode. To disable all the threshold monitoring configuration for a specified IP SLAs operation, use the **no** form of this command.

Syntax Description

operation-number	Number of the IP SLAs operation for which reactions are to be configured.

react *monitored-element* (continued)	• **packetLoss** —Specifies that a reaction should occur if the packet loss value violates the upper threshold or lower threshold. The path of the packets is unknown. • **packetLossDS** —Specifies that a reaction should occur if the one-way destination-to-source packet loss value violates the upper threshold or lower threshold. • **packetLossSD** —Specifies that a reaction should occur if the one-way source-to-destination packet loss value violates the upper threshold or lower threshold. • **rtt** —Specifies that a reaction should occur if the round-trip time violates the upper threshold or lower threshold. • **timeout** —Specifies that a reaction should occur if there is a one-way timeout for the monitored operation. The **threshold-value** keyword does not apply to this monitored element.
action-type *option*	(Optional) Specifies what action or combination of actions the operation performs when threshold events occur. If the **threshold-typenever**keywords are defined, the **action-type** keyword is disabled. The *option* argument can be one of the following keywords: • **none** —No action is taken. This option is the default value. • **trapAndTrigger** —Trigger a Simple Network Management Protocol (SNMP) trap and start another IP SLAs operation when the violation conditions are met, as defined in the **trapOnly** and **triggerOnly** options. • **trapOnly** —Send an SNMP logging trap when the specified violation type occurs for the monitored element. • **triggerOnly** —Transition one or more target operation's operational state from pending to active when the violation conditions are met. The target operations to be triggered are specified using the **ipslareaction-trigger** command.
threshold-type average [*number-of-measurements*]	(Optional) When the average of a specified number of measurements for the monitored element exceeds the upper threshold or when the average of a specified number of measurements for the monitored element drops below the lower threshold, perform the action defined by the **action-type** keyword. For example, if the upper threshold for **reactrttthreshold-typeaverage3** is configured as 5000 ms and the last three results of the operation are 6000, 6000, and 5000 ms, the average would be 6000 + 6000 + 5000 = 17000/3 = 5667, thus violating the 5000 ms upper threshold. The default number of 5 averaged measurements can be changed using the *number-of-measurements* argument. The valid range is from 1 to 16. This syntax is not available if the **connectionLoss**, **timeout**, or **verifyError** keyword is specified as the monitored element, because upper and lower thresholds do not apply to these options.

threshold-type immediate	(Optional) When a threshold violation for the monitored element is met, immediately perform the action defined by the **action-type** keyword.
threshold-value *upper-threshold lower-threshold*	(Optional) Specifies the upper-threshold and lower-threshold values of the applicable monitored elements. See the Default Threshold Values for Monitored Elements table in the "Usage Guidelines" section for a list of the default values. **Note** For MOS threshold values (**reactmos**), the number is expressed in three digits representing ones, tenths, and hundredths. For example, to express a MOS threshold of 3.20, enter **320**. The valid range is from 100 (1.00) to 500 (5.00).

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE `ip sla reaction-configuration` command.

Examples

```
ip sla 7001
 icmp-echo 172.31.17.222 source-ip 172.31.17.216
  request-data-size 64
  tag 7001:AVAILABILITY DSO-D7S
  frequency 30
ip sla schedule 7001 life forever start-time now
ip sla reaction-configuration 6001 react rtt threshold-value 40 40 threshold-type immediate
 action-type trapAndTrigger
ip sla reaction-configuration 6001 react timeout threshold-type immediate action-type
trapAndTrigger
ip sla reaction-configuration 6001 react packetLossDS threshold-value 1 1 threshold-type
immediate action-type trapAndTrigger
ip sla reaction-configuration 6001 react packetLossSD threshold-value 1 1 threshold-type
immediate action-type trapAndTrigger
ip sla reaction-configuration 7001 react timeout threshold-type immediate action-type
trapAndTrigger
```

ip sla responder

To enable the Cisco IOS IP Service Level Agreements (SLAs) Responder for general IP SLAs operations, use the **ip sla responder** command in global configuration mode. To disable the IP SLAs Responder, use the **no** form of this command.

Syntax Description

This command has no arguments or keywords.

Command Default

The IP SLAs Responder is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

This command is used on the destination device for IP SLAs operations to enable the sending and receiving of IP SLAs control packets. Enabling the IP SLAs Responder allows the generation of packet loss statistics on the device sending IP SLAs operations.

Prior to sending an operation packet to the IP SLAs Responder, the IP SLAs operation sends a control message to the IP SLAs Responder to enable the destination port.

For more information about this command, see the Cisco IOS XE `ip sla responder` command.

Examples

The following example shows how to enable the IP SLAs Responder:

```
ip sla responder
```

ip sla schedule

To configure the scheduling parameters for a single Cisco IOS IP Service Level Agreements (SLAs) operation, use the **ip sla schedule**command in global configuration mode. To stop the operation and place it in the default state (pending), use the **no** form of this command.

Syntax Description

operation-number	Number of the IP SLAs operation to schedule.
life forever	(Optional) Schedules the operation to run indefinitely.
life *seconds*	(Optional) Number of seconds the operation actively collects information. The default is 3600 seconds (one hour).
start-time	(Optional) Time when the operation starts.
hh **:** *mm* [**:** *ss*]	Specifies an absolute start time using hour, minute, and (optionally) second. Use the 24-hour clock notation. For example, **start-time 01:02** means “start at 1:02 a.m.,” and **start-time 13:01:30** means “start at 1:01 p.m. and 30 seconds.” The current day is implied unless you specify a *month* and *day*.
month	(Optional) Name of the month to start the operation in. If month is not specified, the current month is used. Use of this argument requires that a day be specified. You can specify the month by using either the full English name or the first three letters of the month.
day	(Optional) Number of the day (in the range 1 to 31) to start the operation on. If a day is not specified, the current day is used. Use of this argument requires that a month be specified.
pending	(Optional) No information is collected. This is the default value.
now	(Optional) Indicates that the operation should start immediately.

after *hh* **:** *mm* **:** *ss*	(Optional) Indicates that the operation should start *hh* hours, *mm* minutes, and *ss* seconds after this command was entered.
random *milliseconds*	(Optional) Adds a random number of milliseconds (between 0 and the specified value) to the current time, after which the operation will start. The range is from 0 to 10000.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE ip sla schedule command.

Examples

```
Device(config)#
```

In the following example, operation 1 begins collecting data after a 5-minute delay:

```
Device(config)# ip sla schedule 1 start-time after 00:05:00
```

In the following example, operation 3 begins collecting data immediately and is scheduled to run indefinitely:

```
Device(config)# ip sla schedule 3 start-time now life forever
```

ip visibility cache entries

To configure the number of entries in IP visibility cache use the **ip visibility cache entries** command. To remove a configured number of entries, use the **no** form of this command.

ip visibility cache entries

Command Default

Disabled.

Command Modes

Policy configuration (config-policy)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

Examples

Enable application-visibility on a router:

```
Router(config)# policy
Router(config-policy)# ip visibility cache entries 20
```

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.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE ipv6 access-list command.

Examples

```
Device# config-transaction
Device(config)# ipv6 access-list test300_v6
Device(config-ip-acl)# sequence 100 permit ipv6 any 2001:DB8::/32
Device(config-ip-acl)#
```

ipv6 visibility cache entries

To configure the number of entries in IPv6 visibility cache use the **ipv6 visibility cache entries** command. To remove a configured number of entries, use the **no** form of this command.

ipv6 visibility cache entries

Command Default

The minimum cache size value is 16. The maximum of total cache size (IPv4 cache + IPv6 cache) should not exceed the limit for each platform. If cache size is not defined and the platform is not in the list, then default maximum cache entries is 200k.

The maximum cache entries is the maximum concurrent flows that Cflowd can monitor. The maximum cache entries vary on different platforms. For more information, contact Cisco Support.

Command Modes

Policy configuration (config-policy)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

Examples

Enable application-visibility on a router:

```
Router(config)# policy
Router(config-policy)# ipv6 visibility cache entries 100
```

jitter

To specify the threshold jitter value that Optimized Edge Routing (OER) will permit for an exit link, use the **jitter** command in OER master controller configuration mode. To reset the maximum jitter value to its default value, use the **no** form of this command.

jitter
no jitter

Command Default

No jitter values are specified.

Command Modes

Policy configuration (config-policy)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates. A app-probe-class keyword is added.

Usage Guidelines

The **jitter** command is used to specify the maximum tolerable jitter value permitted on an exit link. Jitter is a measure of voice quality where the lower the jitter value, the better the voice quality. If the jitter value is greater than the user-defined or the default value, OER determines that the exit link is out-of-policy and searches for an alternate exit link.

Another measure of voice quality is the estimated Mean Opinion Score (MOS). Use the **mos** command and the **jitter** command in an OER policy to define voice quality.

Examples

The following example shows how to configure the master controller to search for a new exit link if the jitter threshold value exceeds 20 milliseconds:

```
Router(config)# oer policy
Router(config-policy-map)# jitter threshold 20
```

lists

To create groupings of similar objects, such as IP prefixes, data-prefixes, and AS paths for use when configuring policy match conditions or action operations, and when to apply a policy, use the **lists** command in the policy configuration mode. To remove the groupings, use the **no lists** form of this command.

lists { **app-list** *app-list-name* | **as-path-list** *path-list* | **community-list** *community-name* | **data-ipv6-prefix-list** *data-prefix-list-name* | **data-prefix-list** *prefix-list-name* | **ext-community-list** *ext-community-name* | **ipv6-prefix-list** *ipv6-prefix-list-name* | **prefix-list** *prefix-list-name* }

no lists { **app-list** *app-list-name* | **as-path-list** *path-list* | **community-list** *community-name* | **data-ipv6-prefix-list** *data-prefix-list-name* | **data-prefix-list** *prefix-list-name* | **ext-community-list** *ext-community-name* | **ipv6-prefix-list** *ipv6-list-name* | **prefix-list** *list-name* }

Syntax Description

app-list *app-list-name*	(Optional) Lists of one or more applications or application families running on the subnets connected to the Cisco IOS XE Catalyst SD-WAN devices. Each app-list can contain either applications or application families, but not both. To configure multiple applications or application families in a single list, include multiple app or app-family options, by specifying one application or application family in each app or app-family option. An application list can contain a mix of applications or application families, but not a mix of the two. We recommend not adding an application to more than one application list, to avoid excessive memory use on devices. Maximum number of application families in an application list: 10
as-path-list *path-list*	(Optional) Lists of one or more BGP AS paths. You can write each AS as a single number or as a regular expression. To specify more than one AS in a single path, include the list in quotation marks (" "). To configure multiple AS paths in a single list, include multiple as-path options, and specifying one AS path in each option.
community-list *community-name*	(Optional) BGP community or communities in the route. list-name is the name of a BGP community list defined with a policy lists community-list command.
data-ipv6-prefix-list *data-prefix-list-name*	(Optional) List of one or more IPv6 prefixes. You can specify both unicast and multicast prefixes. To configure multiple prefixes in a single list, include multiple **ip-prefix** options, specifying one prefix in each option. Does not support: ::/0
data-prefix-list *prefix-list-name*	(Optional) List of one or more prefixes. You can specify both unicast and multicast prefixes. To configure multiple prefixes in a single list, include multiple **ip-prefix** options, specifying one prefix in each option. Does not support: 0.0.0.0/0
ext-community-list *ext-community-name*	(Optional) BGP extended community or communities in the route. Specifies the name of a BGP extended community list defined with a policy lists **ext-community-list** command.
ipv6-prefix-list *ipv6-prefix-list-name*	(Optional) List of one or more IPv6 prefixes. To configure multiple prefixes in a single list, include multiple **ip-prefix** options, specifying one prefix in each option.
prefix-list *prefix-list-name*	(Optional) List of one or more IP prefixes. To configure multiple prefixes in a single list, include multiple **ip-prefix** options, specifying one prefix in each option.

Command Default

None

Command Modes

policy configuration (config-policy)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For more information about this command, see Lists in Localized Policy.

This example defines a data prefix list named Email-Server. The IP prefix of 10.0.0.0/9 is added to the data prefix list Email-Server.

```
Device(config)# policy
Device(config-policy)# lists
Device(config-lists)# data-prefix-list Email-Server
Device(config-config-data-prefix-list-Email-Server)# ip-prefix 10.0.0.0/9
```

This example defines an application list called CollabList, with two applications.

```
Device(config)# policy
Device(config-policy)# lists
Device(config-lists)# app-list CollabList
Device(config-app-list-CollabList)# app ms-office-365
Device(config-app-list-CollabList)# app ms-office-web-apps
```

This example defines an application list called CollabList, with two application families.

```
Device(config)# policy
Device(config-policy)# lists
Device(config-lists)# app-list CollabList
Device(config-app-list-CollabList)# app-family microsoft-office
Device(config-app-list-CollabList)# app-family audio-video
```

This example defines an IPv6 prefix list called PrefixList1.

```
Device(config)# policy
Device(config-policy)# lists
Device(config-lists)# data-ipv6-prefix-list PrefixList1
Device(config-data-ipv6-prefix-list-PrefixList1)# ipv6-prefix 2001:DB8::/32
```

lists data-prefix-list

To configure a list of one or more IP prefixes, use **lists data-prefix-list** command in policy configuration mode. Use the **no** form of this command to remove the list.

lists data-prefix-list *list-name* { **ip-prefix** *prefix/length* }

no lists

data-prefix-list *list-name* **ip-prefix** *prefix/length*	IP Prefix: List of one or more IP prefixes. You can specify both unicast and multicast prefixes. To configure multiple prefixes in a single list, include multiple **ip-prefix** options, specifying one prefix in each option. Does not support: 0.0.0.0/0

Command Default

None.

Command Modes

Policy configuration (config-policy)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

Configure a list of prefixes:

```
Device# policy
Device(config-policy)# lists
Device(config-policy)# data-prefix-list Email-Server
Device(config-policy)# ip-prefix 10.0.0.0/8
```

lists (tag instance)

To create groupings of similar objects within a tag-instance, such as IP prefixes, data-prefixes, and app-lists for use when configuring tag-instances, use the **lists** command in tag-instances configuration mode. To remove the groupings, use the **no** form of this command.

lists [**app-list** *app-list-name*] [**data-ipv6-prefix-list** *data-prefix-list-name*] [**data-prefix-list** *prefix-list-name*]
no lists [**app-list** *app-list-name*] [**data-ipv6-prefix-list** *data-prefix-list-name*] [**data-prefix-list** *prefix-list-name*]

Syntax Description

app-list-name	(Optional) Lists of one or more applications or application families running on the subnets connected to the . Each app-list can contain either applications or application families, but not both. To configure multiple applications or application families in a single list, include multiple app or app-family options, by specifying one application or application family in each app or app-family option.
data-prefix-list-name	(Optional) List of one or more IPv6 prefixes. You can specify both unicast and multicast prefixes. To configure multiple prefixes in a single list, include multiple **ip-prefix** options, specifying one prefix in each option.

prefix-list-name	(Optional) List of one or more prefixes. You can specify both unicast and multicast prefixes. To configure multiple prefixes in a single list, include multiple **ip-prefix** options, specifying one prefix in each option.

Command Default

None

Command Modes

tag-instances configuration (config-tag-instances)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This command was introduced.

Usage Guidelines

Lists configuration under tag-instances are not the same as the lists configured under policy. Tag-instances require their own lists to be configured.

Examples

The following example shows how to configure a data prefix list named pfx1. The IP prefix of 10.20.24.0/24 is added to the data prefix list pfx1:

```
vSmart(config)# tag-instances
vSmart(config-tag-instances)# lists
vSmart(config-lists)# data-prefix-list pfx1
vSmart(config-config-data-prefix-list-pfx1)# ip-prefix 10.20.24.0/24
```

loss

To set the relative or maximum packet loss limit that Optimized Edge Routing (OER) will permit for an exit link, use the **loss** command in OER master controller configuration mode. To return the packet loss limit to the default value, use the **no** form of this command.

loss
no loss

Command Default

OER uses the following default value if this command is not configured or if the no form of this command is entered:

Command Modes

Policy configuration (config-policy)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

The **loss** command is used to specify the relative percentage or maximum number of packets that OER will permit to be lost during transmission on an exit link. If packet loss is greater than the user-defined or the default value, OER determines that the exit link is out-of-policy and searches for an alternate exit link.

The **relative** keyword is used to configure the relative packet loss percentage. The relative packet loss percentage is based on a comparison of short-term and long-term packet loss. The short-term measurement reflects the

percentage of packet loss within a 5-minute period. The long-term measurement reflects the percentage of packet loss within a 60-minute period. The following formula is used to calculate this value:

Relative packet loss = ((short-term loss - long-term loss) / long-term loss) * 100

The master controller measures the difference between these two values as a percentage. If the percentage exceeds the user-defined or default value, the exit link is determined to be out-of-policy. For example, if long-term packet loss is 200 PPM and short-term packet loss is 300 PPM, the relative loss percentage is 50 percent.

The **threshold** keyword is used to configure the absolute maximum packet loss. The maximum value is based on the actual number of PPM that have been lost.

Examples

The following example configures the master controller to search for a new exit link if the difference between long- and short-term measurements (relative packet loss) is greater than 20 percent:

```
Router(config)# oer master
Router(config-oer-mc)# loss relative 200
```

The following example configures OER to search for a new exit link when 20,000 packets have been lost:

```
Router(config)# oer master
Router(config-oer-mc)# loss threshold 20000
```

match (access-control-list)

To enter the match configuration in an access list, use the **match** command in access control list sequence configuration mode. To remove match parameters, use the **no** form of this command.

match [**destination-data-prefix-list** *list-name* | **destination-ip** *ip/length* | **destination-port** *number* | **destination-tag-instance** *dest-tag-name* | **dscp** *number* | **packet-length** *number* | **plp** { **high** | **low** } | **protocol** *number* | **source-data-prefix-list** *list-name* | **source-ip** *ip/length* | **source-port** *number* | **source-tag-instance** *src-tag-name* | **tag-instance** *tag-name* | **tcp syn**]
no match [**destination-data-prefix-list** *list-name* | **destination-ip** *ip/length* | **destination-port** *number* | **destination-tag-instance** *dest-tag-name* | **dscp** *number* | **packet-length** *number* | **plp** { **high** | **low** } | **protocol** *number* | **source-data-prefix-list** *list-name* | **source-ip** *ip/length* | **source-port** *number* | **source-tag-instance** *src-tag-name* | **tcp syn**]

Syntax Description

destination-data-prefix-list *list-name*	(Optional) Matches the specified destination prefix list name.
destination-ip *ip/length*	(Optional) Matches the specified destination IP.
destination-port *number*	(Optional) Matches the specified destination port number. Specify a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-]).
dscp *number*	(Optional) Matches the specified DSCP. The range is from 0 to 63.

packet-length *number*	(Optional) Matches the specified packet length. The range is from 0 to 65535. You can enter a range of values.
plp {**high** | **low** }	(Optional) Matches the specified packet's loss priority (PLP).
protocol *number*	(Optional) Matches the TCP or IP protocol number. The range is from 0 to 255.
source-data-prefix-list *list-name*	(Optional) Matches the specified source prefix list name.
source-ip *IP/length*	(Optional) Matches the specified source IP.
source-port *number*	(Optional) Matches the specified source port number. Specify a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-]).
tcp syn	(Optional) Matches the TCP SYN flag.
source-tag-instance *src-tag-name*	(Optional) Matches the specified source tag instance name. The character range is from 1 to 127.
destination-tag-instance *dest-tag-name*	(Optional) Matches the specified destination tag instance name. The character range is from 1 to 127.

Command Default

None

Command Modes

Access control list sequence configuration (config-sequence-{sequence-number})

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This command was modified. Localized policy match configuration is enhanced to include **source-tag-instance**, and **destination-tag-instance** keyword parameters in matching attributes.

Usage Guidelines

Access control lists (ACLs) perform packet filtering to control which packets move through an interface of a router. Packet filtering provides security by helping to limit network traffic, restrict the access of users and devices to a network, and prevent the traffic from leaving a network interface. An access control list is a sequential list consisting of match-action pairs.

The Sequence Numbering feature applies sequence numbers to match-action pairs. The match–action pairs are evaluated in an order, by sequence number, starting with the lowest numbered pair and ending when it matches the conditions in one of the pairs.

When a packet matches one of the match conditions, the defined action is taken. Or, if no match occurs, the default action is taken.

The **match** command can be used to enter the match configuration mode or to define match parameters.

Examples

The following example shows how to create or enter an access control list named ACL-TEST-1, define sequence #10, specify the destination IP address 10.10.10.10/32 as a match parameter, and define the action to drop when matched:

```
Device(config)# policy
Device(config-policy)# access-list ACL-TEST-1
Device(config-access-list-ACL-TEST-1)# sequence 10
Device(config-sequence-10)# match destination-ip 10.10.10.10/32
Device(config-match)# exit
Device(config-sequence-10)# action drop
```

The following example shows how to configure a localized access control policy to include tags in the matching attributes:

```
Device(config)# policy
Device(config-policy)# access-list acl1
Device(config-access-list-acl1)# sequence 100
Device(config-sequence-100)# match
Device(config-match)# tag-instance orange
Device(config-match)# source-tag-instance red
Device(config-match)# action accept
Device(config-action)# count acl_input_wc
```

The following example shows how to remove destination IP address 10.10.10.10/32 as a match parameter from the access control list ACL-TEST-1, and sequence #10:

```
Device(config)# policy
Device(config-policy)# access-list ACL-TEST-1
Device(config-access-list-ACL-TEST-1)# sequence 10
Device(config-sequence-10)# no match destination-ip 10.10.10.10/32
```

Table 36: Related Commands

Commands	Description
action	Specifies action for matched parameters.
access-list	Configures localized access list policy match.
app-route-policy	Configures centralized application route policy.
data-policy	Configures centralized data policy.
sequence	Configures the sequence number for a match-action pair in an access control list.

match as-path

To match a Border Gateway Protocol (BGP) autonomous system (AS) path access list, use the **match as-path** command. To remove a path list entry, use the **no** form of this command.

match as-path *name*

no match as-path *name*

Syntax Description

name	Autonomous system path access list. You can configure up to 32 access list names.

Command Default

No path lists are defined.

Command Modes

Route-map configuration mode (config-route-map)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

The values set by the **match as-path** command overrides global values.

A route map can have several parts. Any route that does not match at least one **match** clause relating to a **route-map** command is ignored; that is, the route is not advertised for outbound route maps and is not accepted for inbound route maps. If you want to modify some particular data, you must configure a second route-map section with an explicit match specified.

Examples

This example sets the autonomous system path to match BGP autonomous system path access list:

```
Device(config)# route-map rmap1 permit 10
Device(config-route-map)# match as-path 120
```

match (data policy)

To configure matching attributes in a data policy, use the **match** command in data policy sequence configuration mode. To remove match parameters, use the **no** form of this command.

match [**app-list** *app-list-name* | **destination-data-ipv6-prefix-list** *ipv6-prefix-list-name* | **destination-data-prefix-list** *ipv4-prefix-list-name* | **destination-ip** *ip/length* | **destination-port** *number* | **destination-tag-instance** *dest-tag-name* | **dscp** *number* | **packet-length** *number* | **plp** { **high** | **low** } | **protocol** *number* | **source-data-prefix-list** *list-name* | **source-ip** *ip/length* | **source-port** *number* | **source-tag-instance** *src-tag-name* | **tag-instance** *tag-name* | **tcp** **syn**]
no match [**app-list** *app-list-name* | **destination-data-ipv6-prefix-list** *ipv6-prefix-list-name* | **destination-data-prefix-list** *list-name* | **destination-ip** *ip/length* | **destination-port** *number* | **destination-tag-instance** *dest-tag-name* | **dscp** *number* | **packet-length** *number* | **plp** { **high** | **low** } | **protocol** *number* | **source-data-prefix-list** *list-name* | **source-ip** *ip/length* | **source-port** *number* | **source-tag-instance** *src-tag-name* | **tag-instance** *tag-name* | **tcp** **syn**]

Syntax Description

app-list *app-list-name*	(Optional) Matches the specified application list name. The application list name character range is from 1 to 32.
destination-data-ipv6-prefix-list *ipv6-prefix-list-name*	(Optional) Matches the specified destination ipv6 prefix list name. The destination ipv6 prefix list name character range is from 1 to 32.
destination-data-prefix-list *ipv4-prefix-list-name*	(Optional) Matches the specified destination prefix list name. The destination ipv4 prefix list name character range is from 1 to 32.

destination-ip *ipv4 prefix (ip/length)*	(Optional) Matches the specified destination IP.
destination-port *number*	(Optional) Matches the specified destination port number. Specify a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-]). Range: 0 to 65535
dscp *number*	(Optional) Matches the specified DSCP. The range is from 0 to 63.
packet-length *number*	(Optional) Matches the specified packet length. The range is from 0 to 65535. You can enter a range of values.
plp {**high** | **low** }	(Optional) Matches the specified packet's loss priority (PLP).
protocol *number*	(Optional) Matches the TCP or IP protocol number. The range is from 0 to 255.
source-data-prefix-list *list-name*	(Optional) Matches the specified source prefix list name.
source-ip *IP/length*	(Optional) Matches the specified source IP.
source-port *number*	(Optional) Matches the specified source port number. Specify a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-]).
tcpsyn	(Optional) Matches the TCP SYN flag.
traffic-to	(Optional) Matches the specified traffic-to service or access or core.
source-tag-instance *src-tag-name*	(Optional) Matches the specified source tag instance name. The character range is from 1 to 127.
destination-tag-instance *dest-tag-name*	(Optional) Matches the specified destination tag instance name. The character range is from 1 to 127.
tag-instance *tag-name*	(Optional) Matches the specified tag instance name. The character range is from 1 to 127.

Command Default

No match criterion is specified.

Command Modes

Data policy sequence configuration (config-sequence)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This command was introduced.

Usage Guidelines

When a packet matches one of the match conditions, the defined action is taken. Or if no match occurs, the default action is taken.

The **match** command can be used to enter the match configuration mode or to define match parameters.

Examples

The following example shows how to configure centralized data policy to include tags in matching attributes:

```
vSmart(config)# policy
vSmart(config-policy)# data-policy DP1
vSmart(config-data-policy-DP1)# vpn-list vpn1
vSmart(config-vpn-list-vpn1)# sequence 100
vSmart(config-sequence-100)# match
vSmart(config-match)# tag-instance orange
vSmart(config-match)# source-tag-instance red
vSmart(config-match)# destination-tag-instance blue
vSmart(config-match)# action accept
vSmart(config-action)# count count1
```

Table 37: Related Commands

Commands	Description
action	Specifies action for matched parameters.
sequence	To configure the sequence number for a match-action pair in an access control list.
access-list	To configure localized access list policy match.
match (access-control-list)	To configure match attributes in an access list policy.

match ip address

To distribute any routes that have a destination IP network number address that is permitted by a standard access list, an expanded access list, or a prefix list, use the **match ip address** command. To remove the **match ip address** entry, use the **no** form of this command.

match ip address { **prefix-list** | [*prefix-list-name*] }

no match ip address { **prefix-list** | [*prefix-list-name*] }

Syntax Description

prefix-list*prefix-list-name*	Distributes routes based on a prefix list. The prefix list name can be any alphanumeric string up to 63 characters. The ellipsis indicates that multiple values can be entered, up to 32 prefix lists.

Note In Cisco Catalyst SD-WAN Manager Release 20.15.1, when pushing a CLI template to a device running a version earlier than Cisco Catalyst SD-WAN Manager Release 20.15.1, the CLI template must include the following configuration lines under route-map:

```
match ip address prefix-list xyz
match ip address prefix-list-deprecated xyz
match ip address 33
match ip address access-list 33
```

Command Default

No prefix lists are specified.

Command Modes

Route-map configuration mode (config-route-map)

Command History

Note In Cisco Catalyst SD-WAN Manager Release 20.15.1, when pushing a CLI template to a device running a version earlier than Cisco Catalyst SD-WAN Manager Release 20.15.1, the CLI template must include the following configuration lines under route-map:

```
description SET COMMUNITY FOR EDGE ROUTES
description-deprecated SET COMMUNITY FOR EDGE ROUTES
```

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Examples

This example shows how to match routes that have addresses specified by an access list test:

```
Device(config)# route-map rmap1 deny 10
Device(config-route-map)# match ip address prefix-list prfx1
```

match protocol attribute application-group

To configure the match criterion for a class map based on the specified application group, use the **match protocol attribute application-group** command in class-map configuration mode. To remove the application-group match criterion from the class map, use the **no** form of this command.

Supported Parameters

application-group	Name of the application group as a matching criterion. See the "Usage Guidelines" section for a list of application groups supported by most routers.
application-name	(Optional) Name of the application. When the application name is specified, the application is configured as the match criterion instead of the application group.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE `match protocol attribute application-group` command.

Examples

```
class-map match-any ART_APPLICATIONS
 match protocol attribute application-group ms-cloud-group
```

parameter-map type inspect

To configure an inspect-type parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action, use the **parameter-map type inspect** command in global configuration mode. To delete an inspect-type parameter map, use the **no** form of this command.

Syntax Description

parameter-map-name	Name of the inspect parameter map.
global	Defines a global inspect parameter map.
default	Defines a default inspect parameter map.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE parameter-map type inspect command.

Examples

The following example shows the inspect type parameter map configuration:

```
Device(config)# parameter-map type inspect parameter-map type inspect aip
Device(config)# parameter-map type inspect parameter-map type global
```

policer

To define a policer profile and to enter the policer configuration mode, use the **policer** command in policy configuration mode. To remove the policer profile, use the **no** form of this command.

policer *policer-name*
no policer *policer-name*

Syntax Description

policer-name	Name of policer.

Command Default

None

Command Modes

Policy configuration (config-policy)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

To configure policing parameters, create a policer that specifies the maximum bandwidth and burst rate for traffic on an interface, and how to handle traffic that exceeds these values.

This command can be used to define a policer profile and enter the policer configuration mode where further configurations can be done.

Example

The following example defines a policer profile named pol1. It sets the rate to 500,000,000 bps, and burst size to 15,000 bytes, and configures to drop the traffic if the burst size or traffic rate is exceeded.

```
Device(config)# policy
Device(config-policy)# policer pol1
Device(config-policy-pol1)# rate 500000000
Device(config-policy-pol1)# burst 15000
Device(config-policy-pol1)# exceed drop
```

The following example applies a policer using an Access List named ACL-TEST-1.

```
Device(config)# policy
Device(config-policy)# access-list ACL-TEST-1
Device(config-access-list-ACL-TEST-1)# sequence 1
Device(config-sequence-1)# action drop
Device(config-action)# policer pol1
```

Note Rate, burst, and exceed must be defined before committing, otherwise the commit is aborted.

Table 38: Related Commands

Commands	Description
burst	Maximum traffic burst size, in bytes. The range is from 15000 to 10000000.
exceed	Action to take when the burst size or traffic rate is exceeded.

Commands	Description
rate	Bandwidth for 1G interfaces, the range is from 8 to 1000000000 bps; for 10G interfaces, the range is from 8 to 10000000000 bps.

policy

To enter policy configuration mode or configure policies, use the **policy** command in global configuration mode. To remove policy configurations, use the **no** form of this command.

policy [**access-list** | **app-visibility** | **class-map** | **cloud-qos-service-side** | **flow-visibility** | **flow-stickiness-disable** | **implicit-acl-logging** | **ipv6** | **lists** | **log-frequency** | **mirror** | **policer** | **qos-map** | **qos-scheduler** | **rewrite-rule** | **route-policy** | **utd-tls-decrypt**]
no policy [**access-list** | **app-visibility** | **class-map** | **cloud-qos-service-side** | **flow-visibility** | **implicit-acl-logging** | **ipv6** | **lists** | **log-frequency** | **mirror** | **policer** | **qos-map** | **qos-scheduler** | **rewrite-rule** | **route-policy** | **utd-tls-decrypt**]

Syntax Description

access-list	(Optional) Configures ACLs.
app-visibility	(Optional) Enables/disables application visibility.
class-map	(Optional) Configures class map.
cloud-qos	(Optional) Enables/Disables QoS for cEdge Cloud.
cloud-qos-service-side	(Optional) Enables/Disables QoS for cEdge Cloud on service side.
flow-visibility	(Optional) Enables/Disables flow visibility.
flow-stickiness-disable	(Optional) Enables/Disables flow stickiness.
implicit-acl-logging	(Optional) Enables/Disables logging of implicit acl packet drops.
ipv6	(Optional) Configures IPv6 policy.
lists	(Optional) Configures lists.
log-frequency	(Optional) Logs frequency as packet counts.
mirror	(Optional) Configures traffic mirror.
policer	(Optional) Configures policer.
qos-map	(Optional) Configures QoS map.
qos-scheduler	(Optional) Configures QoS scheduler.
rewrite-rule	(Optional) Configures rewrite rule.
route-policy	(Optional) Configures route policies

utd-tls-decrypt	(Optional) Configures TLS Decryption policies.

Command Default

Default behavior or values vary based on optional arguments or keywords.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.
Cisco IOS XE Release 17.6.1a	The **flow-stickiness-disable** keyword is added.
Cisco IOS XE Catalyst SD-WAN Release 17.13.1a	The **flow-stickiness-disable** keyword is added for NAT66 DIA.

Usage Guidelines

Policy influences the flow of data traffic and routing information among Cisco devices in the overlay network. This command can be used to enter the policy configuration mode where further configurations can be done or to configure policies with optional arguments or keywords.

Example

The following example enters the policy configuration mode. It defines a policer profile named pol1 and sets the burst size to 15,000 bytes, and rate to 500,000,000 bps, and configures to drop the traffic if the burst size or traffic rate is exceeded.

```
Device(config)# policy
Device(config-policy)# policer pol1
Device(config-policy-pol1)# burst 15000
Device(config-policy-pol1)# rate 500000000
Device(config-policy-pol1)# exceed drop
Device(config-policy-pol1)# flow-stickiness disable
```

The following example enables app-visibility.

```
Device(config)# policy app-visibility
```

The following example disables flow-stickiness.

```
Device(config-policy)# flow-stickiness disable
```

policy ip visibility

To manually enable or disable policy feature fields visibility, use the **ip visibility** command in policy configuration mode. To disable the feature fields visibility, use the **no** form of the command.

ip visibility features [**cxp** | **dre** | **fec** | **multi-sn** | **pktdup** | **probe-saas** | **sslproxy** | **ulogging**] { *enable* | *disable* }
no ip visibility features [**cxp** | **dre** | **fec** | **multi-sn** | **pktdup** | **probe-saas** | **sslproxy** | **ulogging**] { *enable* | *disable* }

Syntax Description

cxp	cloud express feature

dre	APPQOE DRE feature.
fec	FEC feature
multi-sn	APPQOE Multi SN feature
pktdup	Packet duplicate feature
probe-saas	Probe saas feature
sslproxy	SSLProxy feature
ulogging	Unified logging feature

Command Default

Default behavior or values vary based on optional arguments or keywords.

Command Modes

Policy configuration mode (config-policy)

Command History

Release	Modification
Cisco IOS XE Release 17.9.1a	This command was introduced.

Usage Guidelines

Starting from Cisco IOS XE Release 17.9.1a, you can manually enable or disable the feature fields visibility. Even if the feature fields are enabled automatically due to upgrade, you need to disable fields manually using **ip visibility features** *features***disable** command or use the **no** form of the command.

The disable behavior is same as **no policy ip visibility features**.

The following example shows how to enable the cxp feature fields using the **ip visibility** command:

```
Device(config)# policy ip visibility features cxp enable
```

The following shows how to diable the cxp feature using the **no** form or **disable** command:

```
Device(config)# no policy ip visibility features cxp
Device(config)# policy ip visibility features cxp disable
```

policy log-rate-limit

To limit the number of policy flow logs in a given second, use the **policy log-rate-limit** command in global configuration mode . To disable the limit, use the **no** form of this command.

policy log-rate-limit

This command has no keywords or arguments.

Command Default

The default is 25 messages logged per second.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 17.11.1a	This command was introduced.

Usage Guidelines

The log-rate-limit range is 1 to 10000. For Cisco IOS XE Release 17.11.1a, a maximum rate limit supported is 500.

Example

The following is an example of this command:

```
Device(config)# policy log-rate-limit

(<1..10000> logs per second. Default is 25) (25):
```

The following example shows how to specify a rate limit:

```
Device# show sdwan running-config policy
policy
no app-visibility
no app-visibility-ipv6
no flow-visibility
no flow-visibility-ipv6
no implicit-acl-logging
log-frequency        1000
log-rate-limit    25
access-list ACL1
  sequence 1
   match
    dscp 10
   !
   action accept
    count CNT2
    log
   !
  !
  default-action drop
!
!
```

queue-limit

To specify or modify the maximum number of packets the queue can hold for a class configured in a policy-map, use the **queue-limit** command in policy-map class configuration mode. To remove the queue packet limit from a class, use the **no** form of this command.

queue-limit { *queue-limit-size* { **bytes** | **ms** | **packets** | **us** } **dscp** *dscp-value* }

no queue-limit { *queue-limit-size* { **bytes** | **ms** | **packets** | **us** } **dscp** *dscp-value* }

Syntax Description

queue-limit-size	The maximum size of the queue. Valid range is a number from 1 to 8192000. The maximum varies according to the optional unit of measure keyword specified (bytes, ms, packets, or us).
bytes	(Optional) Indicates that the unit of measure is bytes. Valid range for bytes is a number from 1 to 64000000.
ms	(Optional) Indicates that the unit of measure is milliseconds. Valid range for milliseconds is a number from 1 to 3400.
packets	(Optional) Indicates that the unit of measure is packets. Valid range for packets is a number from 1 to 8192000.
us	(Optional) Indicates that the unit of measure is microseconds. Valid range for microseconds is a number from 1 to 512000.
dscp *dscp-value*	(Optional) Specify the dscp value. Valid options are 0-63, af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs1, cs2, cs3, cs4, cs5, vs6, cs7, default, dscp, ef, precedence.

Command Default

None

Command Modes

Policy-map class configuration (config-pmap-c)

Command History

Release	Modification
	Qualified for use in Cisco vManage CLI templates.

Usage Guidelines

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.

This command can be used to specify or modify the maximum number of packets the queue can hold for a class policy configured in a policy map.

Example

The following example shows defining the maximum queue limit to 108 packets.

```
Router(config)# policy-map POL123
Router(config-pmap)# class CLASS123
Router(config-pmap-c)# bandwidth 1000
Router(config-pmap-c)# queue-limit 108 packets
```

rate

To define the traffic rate for a policer profile, use the **rate** command in policer configuration mode.

rate *bps*

Note Rate is a required parameter in a policer profile. Entering **no rate** *bps* is valid, but causes **commit** to fail.

Syntax Description

bps	Bandwidth for 1G interfaces, the range is from 8 to 1000000000 bps; for 10G interfaces, the range is from 8 to 10000000000 bps.

Command Default

None

Command Modes

Policer configuration (config-policer-{policer-profile-name})

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

To configure policing parameters, create a policer that specifies the maximum bandwidth and burst rate for traffic on an interface, and how to handle traffic that exceeds these values.

This command can be used to define the traffic rate for a policer profile.

Example

The following example defines a policer profile named pol1. It sets the rate to 500,000,000 bps, and burst size to 15,000 bytes, and configures to drop the traffic if the burst size or traffic rate is exceeded.

```
Device(config)# policy
Device(config-policy)# policer pol1
Device(config-policy-pol1)# rate 500000000
Device(config-policy-pol1)# burst 15000
Device(config-policy-pol1)# exceed drop
```

The following example applies a policer using an Access List named ACL-TEST-1.

```
Device(config)# policy
Device(config-policy)# access-list ACL-TEST-1
Device(config-access-list-ACL-TEST-1)# sequence 1
Device(config-sequence-1)# action drop
Device(config-action)# policer pol1
```

Note Rate, burst, and exceed must be defined before committing, otherwise the commit is aborted.

Table 39: Related Commands

Commands	Description
burst	Maximum traffic burst size, in bytes. The range is from 15000 to 10000000.
exceed	Action to take when the burst size or traffic rate is exceeded.

request-data-size

To set the protocol data size in the payload of a Cisco IOS IP Service Level Agreements (SLAs) operation's request packet, use the **request-data-size**command in the appropriate submode of IP SLA configuration, auto IP SLA MPLS configuration, IP SLA monitor configuration, or IP SLA template parameters configuration mode. To return to the default value, use the **no** form of this command.

Syntax Description

bytes	Size of the protocol data in the payload of the request packet of the operation, in bytes. Range is from 0 to the maximum supported by the protocol.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE `request-data-size` command.

IP SLA Configuration

```
ip sla 6001
 udp-jitter 172.31.11.85 44444 source-ip 172.31.17.220 num-packets 100
  request-data-size 64
  tag 6001:UDP64 HNZ-H7Z
  frequency 300
```

rewrite-rule

To configure a rewrite rule to overwrite the DSCP field of a packet's outer IP header, mark transit traffic with an 802.1p CoS value, and apply a rewrite rule on an interface use the **rewrite-rule** command. A rewrite rule is applied to packets that are transmitted out of the interface.

You can apply rewrite rules to both unicast and multicast traffic.

rewrite-rule *rule-name* [**class** *class-name*] { **high** | **low** } **dscp** *dscp-value* **mpls-exp-topmost** *mpls-exp-value*

no rewrite-rule *rule-name* [**class** *class-name*] { **high** | **low** } **dscp** *dscp-value* **mpls-exp-topmost** *mpls-exp-value*

Syntax Description

dscp *dscp-value*	DSCP value: Assign a DSCP value to transit traffic. Range: 0 through 63
mpls-exp-topmost *mpls-exp-value*	Multiprotocol label switching experimental field (MPLS EXP) value: Assign an MPLS EXP value to traffic. **Note** If you use the **dscp** keyword to assign a DSCP value to traffic that uses MPLS, the command maps the DSCP value to an MPLS EXP value using the standard mapping of DSCP to MPLS EXP. For information about this mapping, see the QoS: Classification Configuration Guide, Cisco IOS XE 17. Range: 0 through 7
class *class-name*	Forwarding class name: Name of the forwarding class.
rule-name	Rewrite rule name: Name of the rewrite rule. It can be a text string from 1 through 32 characters long. When you apply a rewrite rule to an interface, the name must match one that you specified when you created the rule with the **policy rewrite-rule** configuration command.

Note Cisco IOS XE SD-WAN supports a maximum number of only 16 rewrite rules and only 64 entries per rewrite rule.

Command Default

None.

Command Modes

Policy configuration (config-policy)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Added the **mpls-exp-topmost** keyword.

Usage Guidelines

For traffic using IP, the **rewrite-rule** command assigns a value to the DSCP field of the IP header for outgoing traffic.

In carrier supporting carrier (CSC) scenarios, which use MPLS, the **rewrite-rule** command assigns the MPLS EXP value in the MPLS header for outgoing traffic. Use the **rewrite-rule** command using a CLI template or CLI add-on template, and the **mpls-exp-topmost** keyword. If, in a CSC scenario, you use the **dscp** keyword

instead, such as with legacy configurations created before support of the **mpls-exp-topmost** keyword, the **rewrite-rule** command converts the DSCP value to an MPLS EXP value in accordance with the standard mapping of DSCP to MPLS EXP values. The benefit of using the **mpls-exp-topmost** keyword is that you can set the MPLS EXP value directly, without depending on the mapping of DSCP to MPLS EXP values.

The following example shows how to create a rewrite rule:

```
Device(config)# policy
Device(config-policy)# rewrite-rule Branch-QoS-Rewrite-Template
Device(config-policy)# class BULK low dscp 10
Device(config-policy)# class BULK high dscp 10
```

The following example applies to a CSC scenario. It defines a rewrite rule called rw-exp, which sets the MPLS EXP value for outgoing traffic to 1 and applies the rule to the outbound interface.

Define the rewrite rule using the **mpls-exp-topmost** keyword, as follows:

```
sdwan
  policy
    rewrite-rule rw-exp
      class BULK low mpls-exp-topmost 1
      class BULK high mpls-exp-topmost 1
```

Alternatively, if you define the rewrite rule using the **dscp** keyword, the **rewrite-rule** command converts the value of 10 to an MPLS EXP value of 1, in accordance with the standard mapping of DSCP to MPLS EXP values.

```
sdwan
  policy
    rewrite-rule rw-exp
      class BULK low dscp 10
      class BULK high dscp 10
```

Apply the rule as follows:

```
sdwan
interface GigabitEthernet0/0/2
  tunnel-interface
   encapsulation ipsec weight 1
   no border
   color public-internet restrict
  exit
  rewrite-rule rw-exp
exit
```

service-area

To classify traffic based on service areas for different Microsoft 365 (M365) cloud services, use the **service-area** command in Policy configuration (config-policy) mode.

service-area *service-area-name*

no service-area *service-area-name*

Syntax Description

service-area name	Specifies one or more service-areas that the M365 cloud application belongs to. The four service areas are: • **Common**: M365 Pro Plus, Office in a browser, Azure AD, and other common network endpoints. • **Exchange**: Exchange Online and Exchange Online Protection. • **SharePoint**: SharePoint Online and OneDrive for Business. • **Skype**: Skype for Business and Microsoft Teams.

Command Default

There are no default values.

Command Modes

Policy configuration (config-policy)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

- SD-AVC must be enabled on Cisco vManage.
- You can add only one sequence with a match for a service-area, to a policy configuration in Cisco vManage.

The following example shows how to specify a service area:

```
policy
 app-route-policy test_policy
  vpn-list vpn-list-1
   sequence 111
    match
     source-ip 0.0.0.0/0
     service-area exchange sharepoint skype
     traffic-category optimize-allow
    !
    action
     count count-name
     cloud-saas
    !
   !
  !
```

service-policy

To attach a policy map to an input interface, a virtual circuit (VC), an output interface, or a VC that will be used as the service policy for the interface or VC, use the **service-policy** command in the appropriate configuration mode. To remove a service policy from an input or output interface or from an input or output VC, use the **no** form of this command.

Supported Parameters

type	(Optional) Determines the exact pattern to look for in the protocol stack of interest.
input	Attaches the specified policy map to the input interface or input VC.
policy-map-name	The name of a service policy map (created using the **policy-map** command) to be attached. The name can be a maximum of 40 alphanumeric characters in length.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `service-policy` command.

Examples

```
interface GigabitEthernet0/0/1
 service-policy type epbr input test300
interface GigabitEthernet0/0/2
 service-policy type epbr input test100
```

set ip vrf

To indicate where to forward packets that pass a match clause of a route map for policy routing when the next hop must be under a specified virtual routing and forwarding (VRF) name, use the **setipvrf** command in policy map class configuration mode. To disable this feature, use the **no** form of this command.

Supported Parameters

vrf-name	Name of the VRF.
next - hop *ip-address*	IP address of the next hop to which packets are forwarded. The next hop must be an adjacent router.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `set ip vrf` command.

Examples

```
ip access-list extended test300
 100 permit ip any 0.0.0.2 255.255.255.0
ip access-list extended test100
 100 permit ip any 0.0.0.2 255.255.255.0
class-map match-any test300
 match access-group name test300
```

```
class-map match-any test100
 match access-group name test100
policy-map type epbr test300
 class test300
  set ipv4 vrf 300 next-hop 203.0.113.255
policy-map type epbr test100
 class test100
  set ipv4 vrf 100 next-hop 203.0.113.255
interface GigabitEthernet0/0/1
 service-policy type epbr input test300
interface GigabitEthernet0/0/2
 service-policy type epbr input test100
```

```
ipv6 access-list test300_v6
  sequence 100 permit ipv6 any 2003::2/64
ipv6 access-list test100_v6
 sequence 100 permit ipv6 any 2001::2/64
class-map match-any test300_v6
 match access-group name test300_v6
class-map match-any test100_v6
 match access-group name test100_v6
policy-map type epbr test300_v6
 class test300_v6
  set ipv6 vrf 300 next-hop 2003::2
policy-map type epbr test100_v6
 class test100_v6
  set ipv6 vrf 100 next-hop 2001::2
interface GigabitEthernet0/0/1
 service-policy type epbr input test300_v6
interface GigabitEthernet0/0/2
 service-policy type epbr input test100_v6
```

set ip next-hop verify-availability

To configure policy routing to verify the reachability of a single or multiple IPv4 or IPv6 next hops of a policy map before the router performs policy routing to the next hops, use the **set ipv4 next-hop verify-availability** or **set ipv6 next-hop verify-availability** commands respectively in the policy-map class mode.

To disable this feature, use the **no** form of this command

set [**ipv4** | **ipv6**] [**vrf** *vrf-name* | **global**] **next-hop verify-availability** [*ip-address* ... [*ip-address*]] [*nhop-address sequence* **track** *object-number*]
no [**ipv4** | **ipv6**] [**vrf** *vrf-name* | **global**] **next-hop verify-availability** [*ip-address* ... [*ip-address*]] [*nhop-address sequence* **track** *object-number*]

Syntax Description

vrf *vrf-name*	Specifies that the next hop reachability should be verified for a specific VRF.
global	Specifies that the next hop reachability should be verified at a global level
ip-addresses	Specifies a single or multiple next hops addresses to verify their reachability
nhop-address	Specifies a single next hop address to verify its reachability
sequence	Specifies the sequence to be inserted into the next-hop list. The range is from 1 to 65535.
track	Sets the next hop depending on the state of a tracked object.

object-number	Specifies tracked object number. The range is from 1 to 1000.

Command Default

This command s disabled by default.

Command Modes

Policy-map class configuration (config-pmap-c)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	This command was introduced.

Usage Guidelines

Use this command to enable policy routing to verify the reachability of a single or multiple IPv4 or IPv6 next hop addresses. This command can be configured globally or for a vrf. The options after **set [ipv4|ipv6] next-hop verify-availability** can be configured in any order.

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the ip-address argument

Example

The following example shows how to verify the availability of an IPv4 next hop address, and enable tracker for the address.

```
Device(config)# class-map match-any test100

Device(config-cmap)# match acess-group name test100

Device(config-cmap)# policy-map type epbr 1

Device(config-pmap)# class test300

Device(config-pmap-c)# set ipv4 vrf 300 next-hop verify-availability 10.10.0.2 10 track 2
```

The following example shows how to verify the availability of an IPv6 next hop address and enable tracker for the address.

```
Device(config)# class-map match-any test100_v6

Device(config-cmap)# match acess-group name test100_v6

Device(config-cmap)# policy-map type epbr test300_v6

Device(config-pmap)# class test300_v6

Device(config-pmap-c)# set ipv6 vrf 300 next-hop verify-availability 2001:DB8::1 10 track
4
```

sequence

To specify a sequence number for the permit condition in the IP access list, use the **sequence** command in the appropriate configuration mode. To remove a sequence number from an IP access list, use the **no** form of this command.

sequence *sequence-number* { **permit** } { **ipv6** } { **any** *ipv6-address* }

Syntax Description

sequence-number	Permits statements to position the statement in the list.
permit	Sets permit conditions for an IPv6 access list.
ipv6	Sets the IPv6 address to set permit conditions.
any *ipv6-address*	Specifies any source or any destination host as an abbreviation for the *source-addr* or *destination-addr value* and the *source-wildcard* or *destination-wildcard* value of 0.0.0. 255.255.255.255.

Command Default

There are no specific conditions under which a packet passes the access list.

Command Modes

IPv6 access-list configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

Examples

```
Device(config)# ipv6 access-list test300_v6
Device(config-ipv6-acl)# sequence 100 permit ipv6 any 2001:DB8::/32
```

sequence (access-control-list)

To define the sequence number for a match-action pair in an access control list, use the **sequence** command in access control list configuration mode. To remove the sequence number and match-action pair, use the **no** form of this command.

sequence *number*
no sequence *number*

Syntax Description

number	Sequence number ranging from 0 to 65535.

Command Default

None

Command Modes

Access Control List configuration (config-access-list-{ACL-name})

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Access control lists (ACLs) perform packet filtering to control which packets move through an interface of a router. The packet filtering provides security by helping to limit the network traffic, restrict the access of

users and devices to a network, and prevent the traffic from leaving a network interface. An access control list is a sequential list consisting of match-action pairs.

The sequence numbering feature applies sequence numbers to match-action pairs. The match–action pairs are evaluated in order, by sequence number, starting with the lowest numbered pair and ending when it matches the conditions in one of the pairs.

When a packet matches one of the match conditions, the defined action is taken. Or if no match occurs, the default action is taken.

This command can be used to define the sequence number for a match-action pair in an access control list.

Example

The following example creates an access control list named ACL-TEST-1, defines sequence #10, specifies destination IP 10.10.10.10/32 as a match parameter and defines the action to drop when matched.

```
Device(config)# policy
Device(config-policy)# access-list ACL-TEST-1
Device(config-access-list-ACL-TEST-1)# sequence 10
Device(config-sequence-10)# match destination-ip 10.10.10.10/32
Device(config-match)# exit
Device(config-sequence-10)# action drop
```

The following example creates an access control list named ACL-TEST-1 and removes sequence #10 and the match-action pair.

```
Device(config)# policy
Device(config-policy)# access-list ACL-TEST-1
Device(config-access-list-ACL-TEST-1)# no sequence 10
```

Table 40: Related Commands

Commands	Description
default-action	Specifies default action for matched parameters.

sla-class

To configure a Service Level Agreements (SLA) class, use the **sla-class** command in global configuration mode. You can create groups of properties for a policy to use with application-aware routing. You can configure a maximum of six SLA classes for Cisco IOS XE SD-WANs.

sla-class *sla-class-name* **jitter** *jitter* **latency** *latency* **loss** *percentage* **app-probe-class** *app-probe-class-name* [**fallback-to-best-tunnel criteria** *criteria* **jitter** *jitter* **latency** *latency* **loss** *percentage*]

no sla-class *sla-class-name*

Syntax Description

jitter *milliseconds*	Specifies the jitter on the connection. Packets matching the policy for application-aware routing that have the specified jitter or a lower jitter value. *Range:* 1 through 1000 milliseconds

latency *milliseconds*	Specifies the latency on the connection. Packets matching the policy for application-aware routing that have the specified latency or a lower latency value. *Range:* 1 through 1000 milliseconds
loss *percentage*	Specifies the packet loss on the connection. Packets matching the policy for application-aware routing that have the specified packet loss or a lower packet loss value. *Range:* 0 through 100 percentage
app-probe-class *app-probe-class-name*	Specifies the app-probe-class configured on the SLA class.
(Optional) **fallback-to-best-tunnel**	(Optional) Specifies the fallback-to best-tunnel option. When this option is selected, the packet can choose the best path available using the criteria.
criteria	Specifies the criteria. The options are a combination of one or more of loss, latency, and jitter values.

Command Default

There are no default values.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates. A app-probe-class keyword is added.
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	A fallback-best-tunnel and criteria keywords are added.

The following example shows the SLA configuration for a latency of 50 millisecond and a app-probe-class along with the fallback-best-tunnel option:

```
Device(config)# policy
Device(config-policy)# sla-class 50ms-sla
Device(config-policy))# latency 50
Device(config-policy))# app-probe-class real-time-video
Device(config-policy))# fallback-best-tunnel
Device(config-policy))# criteria loss jitter
```

sig

To enable VPN multiplexing and demultiplexing, use the **sig** command in the action configuration mode. The SIG tunnel is created in the VPN 0 (global) space. The SIG tunnel configuration is identical to other

IPSEc tunnel configurations, excluding the inclusion of the **tunnel vrf multiplexing** command. To remove the multiplexing, use the **no sig** form of this command.

sig

no sig

Syntax Description This command has no arguments or keywords.

Command Default No default behavior or values.

Command Modes action configuration (config-action)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

```
vSmart(config)# policy
vSmart(config-policy)# data-policy sig_ha_zscaler_data_policy_cedge
vSmart(config-data-policy-sig_ha_zscaler_data_policy_cedge)# vpn-list vpn_1
vSmart(config-vpn-list-vpn_1)# sequence 100
vSmart(config-sequence-100)# match destination-ip 10.10.10.10/32
vSmart(config-match)# protocol 17
vsmart(config-match)# !
vsmart(config-match)# action accept
vsmart(config-action)# count sig_ha_zscaler_datapolicycnt100
vsmart(config-action)# sig
vsmart(config-action)# exit
vsmart(config-action)# exit
```

site-list

To list of one or more identifiers of sites in the Cisco SD-WAN overlay network, use the **site-list** command in the policy lists configuration mode. To remove the listing of sites, use the **no site-list** form of this command.

site-list *list-name*

no site-list *list-name*

Syntax Description

list-name	List of sites to which to apply the policy. The *list-name* must match a list name that you configured in the **policy lists site-list** part of the configuration.

Command Default None

Command Modes policy lists configuration (config-lists)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

The following example configures site lists to use for control and data policies that contain overlapping site identifiers, and apply the policies to this site lists on a Cisco vSmart Controller.

```
vSmart(config)# policy
vSmart(config-policy)# lists
vSmart(config-lists)# site-list us-control-list
vSmart(config-lists)# site-id 1-200
vSmart(config-lists)# site-list emea-control-site-list
vSmart(config-lists)# site-id 201-300
vSmart(config-lists)# site-list apac-control-site-list
vSmart(config-lists)# site-id 301-400
```

tag (IP SLA)

To create a user-specified identifier for a Cisco IOS IP Service Level Agreements (SLAs) operation, use the **tag** (IP SLA) command in the appropriate submode of IP SLA configuration, auto IP SLA MPLS configuration, or IP SLA monitor configuration mode. To remove a tag from an operation, use the **no** form of this command.

Syntax Description

text	Name of a group to which the operation belongs from 0 to 16 ASCII characters.

Command Default

No tag identifier is specified.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE `tag` command.

```
ip sla responder
ip sla 6001
 udp-jitter 172.31.11.85 44444 source-ip 172.31.17.220 num-packets 100
  request-data-size 64
  tag 6001:UDP64 HNZ-H7Z
  frequency 300
ip sla schedule 6001 life forever start-time now
ip sla 7001
 icmp-echo 172.31.17.222 source-ip 172.31.17.216
  request-data-size 64
  tag 7001:AVAILABILITY DSO-D7S
  frequency 30
ip sla schedule 7001 life forever start-time now
ip sla reaction-configuration 6001 react rtt threshold-value 40 40 threshold-type immediate
 action-type trapAndTrigger
ip sla reaction-configuration 6001 react timeout threshold-type immediate action-type
trapAndTrigger
ip sla reaction-configuration 6001 react packetLossDS threshold-value 1 1 threshold-type
immediate action-type trapAndTrigger
```

```
ip sla reaction-configuration 7001 react timeout threshold-type immediate action-type
trapAndTrigger
```

tag-instances

To configure tag instances with member attributes, use the **tag-instances** command in global configuration mode. To delete the tag instances, use the **no** form of this command.

tag-instances tag-instance *tag-instance-name* [**app-list** *app-list-name*] [**data-prefix-list** *data-prefix-list-name*] [**data-ipv6-prefix-list** *ipv6-prefix-list-name*] [**id** *tag-id*]
no tag-instances tag-instance *tag-instance-name*

Syntax Description

tag-instance	Specifies the tag instance information.
tag-instance-name	Specifies the tag instance name.
app-list-name	Specify the list of app list names of 1 to 32 characters.
data-prefix-list-name	Specify the list of data prefix list names of 1 to 32 characters.
data-ipv6-prefix-list-name	Specify the list of data IPv6 prefix list names of 1 to 32 characters.
tag-id	Global unique ID assigned to each of the tag instances. Range: 1 to 4294967295.

Command Default

No tag identifier is specified.

Command Modes

Global configuration mode (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This command was introduced.

Usage Guidelines

You cannot modify the tag ID after the tag name is provided. To modify a tag ID, delete the tag and create a new tag with a new tag ID.

Examples

The following example shows how to configure tag-instances red and blue with unique tag-ids and data-prefix-list names:

```
tag-instances
 tag-instance red
  tag-id 1000
  data-prefix-list pfx1 pfx2
!
 tag-instance blue
  tag-id 2000
  data-ipv6-prefix-list v6_pfx1 v6_pfx2
!
```

Related Commands

Command	Description
lists	To create groupings of similar objects, such as IP prefixes, data-prefixes, and app-lists for use when configuring tag-instances. Note that the lists configured under tag-instances is not same as the lists configured under policy. Tag-instances requires its own lists configured.

track ip sla

To track the state of a Cisco IOS IP Service Level Agreements (SLAs) operation and to enter tracking configuration mode, use the **track ip sla** command in global configuration mode. To remove the tracking, use the **no** form of this command.

track ip *jitter* **sla**

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE track ip sla command.

Note In Cisco Catalyst SD-WAN Manager Release 20.15.1, when pushing a CLI template to a device running a version earlier than Cisco Catalyst SD-WAN Manager Release 20.15.1, the CLI template must add another command, **track tracked-object** *track-id* **ip sla** *ip sla-id* **state**.

```
track 1 ip sla 2 state
track tracked-object 1 ip sla 2 state
```

Examples

The following example shows how to configure the tracking process to track the state of IP SLAs operation 2:

```
Device(config)# track 1 ip sla 2 state
Device(config-track)
```

The following example shows how to configure the tracking process to track the reachability of IP SLAs operation 3:

```
Device(config)# track 2 ip sla 3 reachability
Device(config-track)
```

udp-jitter

To configure a Cisco IOS IP Service Level Agreements (SLAs) User Datagram Protocol (UDP) jitter operation or a IP SLAs multicast UDP jitter operation and enter UDP jitter or multicast UDP jitter configuration mode, use the **udp-jitter**command in IP SLA configuration mode.

Syntax Description

destination-ip-address | *destination-hostname*	Destination IPv4 or IPv6 address or hostname. • For a multicast UDP jitter operation, this must be a multicast IP address.
destination-port	Specifies the destination port number. The range is from 1 to 65535.
source-ip {*ip-address* | *hostname*}	(Optional) Specifies the source IPv4 or IPv6 address or hostname. When a source IP address or hostname is not specified, IP SLAs chooses the IP address nearest to the destination.
num-packets *number-of-packets*	(Optional) Specifies the number of packets. The default is 10.

Command Default

No IP SLAs operation type is configured for the operation being configured.

Command Modes

IP SLA configuration (config-ip-sla)

Command History

Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco vManage CLI templates..

Usage Guidelines

For more information about this command, see the Cisco IOS XE `udp-jitter` command.

Examples

```
ip sla responder
ip sla 6001
 udp-jitter 172.31.11.85 44444 source-ip 172.31.17.220 num-packets 100
  request-data-size 64
  tag 6001:UDP64 HNZ-H7Z
  frequency 300
ip sla schedule 6001 life forever start-time now
ip sla 7001
 icmp-echo 172.31.17.222 source-ip 172.31.17.216
  request-data-size 64
  tag 7001:AVAILABILITY DSO-D7S
  frequency 30
ip sla schedule 7001 life forever start-time now
ip sla reaction-configuration 6001 react rtt threshold-value 40 40 threshold-type immediate
 action-type trapAndTrigger
ip sla reaction-configuration 6001 react timeout threshold-type immediate action-type
trapAndTrigger
ip sla reaction-configuration 6001 react packetLossDS threshold-value 1 1 threshold-type
immediate action-type trapAndTrigger
ip sla reaction-configuration 7001 react timeout threshold-type immediate action-type
trapAndTrigger
```

utd-policy

To attach an Unified Threat Defense (UTD) action to a policy, use the **utd-policy** command in profile configuration mode.The UTD action contains both the UTD profile and a UTD policy that will be applied, and along with the TLS decryption action.

utd-policy *policy-name*

Syntax Description

policy-name	Enter a name for the UTD policy.

Command Modes

Profile configuration (config-profile)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Qualified for use in Cisco vManage CLI templates

The following example shows how to attach a profile for a Unified Security Policy.

```
Device(config)# parameter-map type inspect aip
Device(config-profile)# utd-policy united
```

vpn-list

To list the VPNs on Cisco vSmart Controllers for which a policy is applicable such as, data-policy and app-route-policy, use the **vpn-list** command in data policy configuration mode. To remove the list of VPNs, use the **no** form of this command.

vpn-list { *list-name* }

no vpn-list { *list-name* }

Syntax Description

list-name	Specifies the name of the policy-related list that the Cisco vSmart Controller saves on the Cisco IOS XE Catalyst SD-WAN device.

Command Default

None

Command Modes

data policy configuration (config-data-policy)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For more information about this command, see Centralized Policy.

```
vSmart(config)# policy
vSmart(config-policy)# data-policy sig_ha_zscaler_data_policy_cedge
vSmart(config-data-policy-sig_ha_zscaler_data_policy_cedge)# vpn-list vpn_1
vSmart(config-vpn-list-vpn_1)# sequence 100
vSmart(config-sequence-100)# match destination-ip 10.10.10.10/32
vSmart(config-match)# protocol 17
vsmart(config-match)# !
vsmart(config-match)# action accept
vsmart(config-action)# count sig_ha_zscaler_datapolicycnt100
vsmart(config-action)# sig
vsmart(config-action)# exit
vsmart(config-action)# exit
vSmart(config-vpn-list-vpn_1)# sequence 110
vSmart(config-sequence-110)# match app-list googel_app
vSmart(config-match)# destination-data-prefix-list dest_prefix_list
vsmart(config-match)# !
vsmart(config-match)# action accept
vsmart(config-action)# count sig_ha_zscaler_datapolicycnt110
vsmart(config-action)# sig
vsmart(config-action)# exit
vsmart(config-action)# exit
vSmart(config-vpn-list-vpn_1)# sequence 120
vSmart(config-sequence-110)# match app-list amazon
vSmart(config-match)# destination-data-prefix-list dest_prefix_list
vsmart(config-match)# !
vsmart(config-match)# action accept
vsmart(config-action)# count sig_ha_zscaler_datapolicycnt120
vsmart(config-action)# sig
vsmart(config-action)# exit
vsmart(config-action)# exit
vSmart(config-sequence-120)# default-action accept
```

vrf (IP SLA)

To allow monitoring within Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs) using Cisco IOS IP Service Level Agreements (SLAs) operations, use the **vrf** command in the appropriate submode of IP SLA configuration, IP SLA monitor configuration, or IP SLA template configuration mode.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE vrf (IP SLA) command.

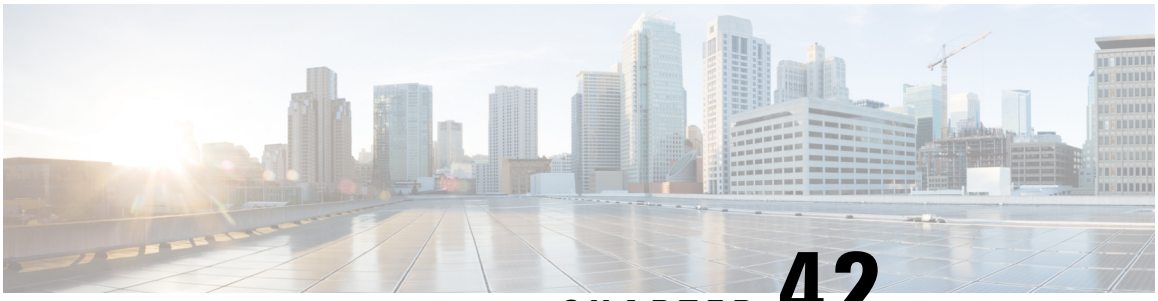
Examples

The following examples show how to configure an IP SLAs operation for an MPLS VPN. These examples show how test traffic can be sent in an already existing VPN tunnel between two endpoints.

IP SLA Configuration

```
Device# config-transaction
Device(config)# ip sla 1
Device(config-ip-sla)# icmp-echo 10.1.1.1
```

```
Device(config-ip-sla-echo)# vrf vpn1
Device(config-ip-sla-echo)#
```



CHAPTER 42

PPP Commands

- encapsulation, on page 619
- encapsulation (ATM), on page 620
- ppp authentication, on page 622
- ppp chap hostname, on page 623
- ppp chap password, on page 624
- ppp ipcp, on page 624
- pvc, on page 625

encapsulation

To set the encapsulation method used by the interface, use the **encapsulation** command in interface configuration mode. To remove the encapsulation, use the **no** form of this command.

encapsulation *encapsulation-type*
no encapsulation *encapsulation-type*

Syntax Description

encapsulation-type	Encapsulation type; one of the following keywords: • **dot1q** *vlan-id* ---Enables IEEE 802.1q encapsulation of traffic on a specified subinterface in VLANs. The *vlan-id* argument is a virtual LAN identifier. • **frame-relay** --Frame Relay (for serial interface). • **ppp** -- PPP (for Dialer interface).

Command Default

NA

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates. The following keywords are qualified: • **dot1q** for GigabitEthernet interface . • **ppp** for Dialer interface.
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Command qualified for use in Cisco vManage CLI templates. The following keywords are qualified: • **encapsulation frame-relay** for serial interface.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE encapsulation command.

Examples

The following example shows how to enable frame-relay encapsulation on Serial interface 0:

```
Device(config)# interface Serial 0
Device(config-if)# encapsulation frame-relay
```

The following example shows how to configure Dialer interface 1 for PPP encapsulation:

```
Device(config)# interface Dialer 1
Device(config-if)# encapsulation ppp
```

encapsulation (ATM)

To configure the ATM adaptation layer (AAL) and encapsulation type for an ATM virtual circuit (VC), VC class , VC, bundle, or permanent virtual circuit (PVC) range, use the **encapsulation**command in the appropriate mode. To remove an encapsulation type, use the **no** form of this command.

encapsulation { **aal5mux** *protocol* | **aal5snap** }

no encapsulation

Syntax Description

aal5mux	Specifies the AAL and encapsulation type for multiplex (MUX)-type VCs. A protocol must be specified when you use this encapsulation type.

protocol	Protocol type being used by the multiplex (MUX)-encapsulated VC. Values for the *protocol*argument are as follows: • **appletalk** --AppleTalk protocol. • **bridge ieee8023** --Ethernet LAN protocol. • **decnet** --DECnet protocol. • **frame-relay** --Frame Relay-ATM Network Interworking (FRF.5) on the Cisco MC3810. • **fr-atm-srv** --Frame Relay-ATM Service Interworking (FRF.8) on the Cisco MC3810. • **ip** --IP protocol. • **ipx** --Internet Packet Exchange (IPX) protocol. • **ppp Virtual-Template** *template-number* - Internet Engineering Task Force (IETF)-compliant PPP over ATM. Use the **virtual-template** *template-number* option to identify the virtual template. This keyword is supported on ATM PVCs only. • **pppoe** --PPP over Ethernet. • **voice** --Voice over ATM.
aal5snap	Specifies the AAL and encapsulation type that supports Inverse Address Resolution Protocol (ARP). Logical link control/Subnetwork Access Protocol (LLC/SNAP) precedes the protocol datagram.

Command Default

The global default encapsulation option is **aal5snap**.

Command Modes

ATM PVC configuration (config-if-pvc)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates. The **aal5snap** command option is qualified.
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Command qualified for use in Cisco vManage CLI templates. The **aal5mux** *protocol* command option is qualified.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `encapsulation (ATM)` command.

MUX-Type Encapsulation on a VC Example

```
Device(config)# interface ATM 0/3/0
Device(config-subif)# no shutdown
Device(config-subif)# pvc 0/1
Device(config-if-pvc)# encapsulation aal5mux ppp Virtual-Template 1
```

SNAP Encapsulation Example

```
Device(config)# interface ATM 0/3/0.1 point-to-point

Device(config-subif)# ip address 10.0.0.0 255.255.255.252
Device(config-subif)# ip mtu 1496
Device(config-subif)# no shutdown
Device(config-subif)# pvc 0/100
Device(config-if-pvc)# bridge-dot1q encap 1
Device(config-if-pvc)# encapsulation aal5snap
```

MUX Encapsulation Example

```
Device(config)# interface ATM 0/2/0.1 point-to-point
Device(config-subif)# pvc 0/1
Device(config-if-pvc)# encapsulation aal5mux ppp dialer
```

ppp authentication

To enable at least one PPP authentication protocol and to specify the order in which the protocols are selected on the interface, use the **ppp authentication** command in interface configuration mode. To disable this authentication, use the **no**form of this command.

ppp authentication *protocol1* [*protocol2...*] [**callin**]
no ppp authentication

Syntax Description

protocol1 [*protocol2...*]	At least one of the following keywords: • **chap** : Enables CHAP on a dialer interface. • **pap** : Enables PAP on a dialer interface.
callin	(Optional) Authentication on incoming (received) calls only.

Command Default

PPP authentication is not enabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates. The following command is qualified: **ppp authentication chap callin**
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Command qualified for use in Cisco vManage CLI templates. The following command is qualified: **ppp authentication** {**chap** | **pap** | **chap pap**} [**callin**]

Usage Guidelines

For usage guidelines, see the Cisco IOS XE ppp authorization command.

Examples

```
Device(config)# interface Dialer 1
Device(config-if)# encapsulation ppp
Device(config-if)# ppp authentication chap callin
```

```
Device(config)# interface Dialer 1
Device(config-if)# encapsulation ppp
Device(config-if)# ppp authentication chap pap callin
```

ppp chap hostname

To create a pool of dialup routers by specifying a common alias for all routers when authenticating with CHAP (Challenge Handshake Authentication Protocol), use the **ppp chaphostname** command in interface configuration mode. To disable this function, use the no form of the command.

ppp chap hostname *hostname*
no ppp chap hostname

Syntax Description

hostname	The name sent in the CHAP challenge.

Command Default

Disabled. The router name is sent in any CHAP challenges.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

The command is available only when **encapsulation ppp** is configured.

The **ppp chap hostname** command allows you to specify a common alias for all routers in a rotary group to use so that only one username must be configured on the dialing routers.

This command is normally used with local CHAP authentication (when the router authenticates to the peer), but it can also be used for remote CHAP authentication.

Note By default, after changing hostnames, an MLP member link does not undergo failure recovery automatically. You must use the **ppp chap hostname** command to define the Multilink PPP (MLP) bundle name on an endpoint. If this command is not configured and the hostname is changed, then a link flap will not return the link back to the bundle.

Examples

```
Device(config)# interface Dialer 1
Device(config-if)# encapsulation ppp
Device(config-if)# ppp chap hostname ntt
```

ppp chap password

To configure a common CHAP secret to be used in responses to challenges from an unknown remote peer in a collection of routers that do not support this command (such as routers running older Cisco IOS software images), use the **ppp chap password** interface configuration command. To disable this function, use the **no** form of this command.

ppp chap password *secret*
no ppp chap password *secret*

Syntax Description

secret	The secret used to compute the response value for any CHAP challenge from an unknown peer.

Command Default

Disabled

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

The command is available only when **encapsulation ppp** is configured.

This command allows you to replace several username and password configuration commands with a single copy of this command on any dialer interface or asynchronous group interface.

This command is used for remote CHAP authentication only (when routers authenticate to the peer) and does not affect local CHAP authentication.

Examples

```
Device(config)# interface Dialer 1
Device(config-if)# encapsulation ppp
Device(config-if)# ppp chap password ntt
```

ppp ipcp

To configure PPP IP Control Protocol (IPCP) features such as the ability to provide primary and secondary Domain Name Server (DNS) and Windows Internet Naming Service (WINS) server addresses, and the ability to accept any address requested by a peer, use the **ppp ipcp** command in template or interface configuration mode. To disable a PPP IPCP feature, use the no form of this command.

ppp ipcp { **dns request** | **mask request** }
no ppp ipcp

Syntax Description

dnsrequest	Requests the DNS address from the peer.
maskrequest	Requests the subnet mask from the peer.

Command Default No servers are configured, and no address request is made.

Command Modes

Template configuration
Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 17.5.1a	Command qualified for use in Cisco vManage CLI templates.

Examples

The following examples show use of the **ppp ipcp** command:

```
Device(config)# interface Dialer1
Device(config-if)# ppp ipcp dns request
Device(config-if)# ppp ipcp mask request
```

The following examples show how to use the **no** form of the **ppp ipcp** command:

```
no ppp ipcp
```

pvc

To create or assign a name to an ATM permanent virtual circuit (PVC), to specify the encapsulation type on an ATM PVC, and to enter ATM virtual circuit configuration mode, use the **pvc** command in interface configuration mode or subinterface configuration mode. To remove an ATM PVC from an interface, use the **no** form of this command.

pvc *vpi/vci*

Syntax Description

vpi	Specifies the ATM network virtual path identifier (VPI) for this PVC. The slash is required. This value defaults to 0 if no value is given for *vpi/*. The arguments *vpi* and *vci* cannot both be set to 0; if one is 0, the other cannot be 0.
vci	Specifies the ATM network virtual channel identifier (VCI) for this PVC. The range of valid values is 0 to 1 less than the maximum value set for this interface by the atm vc-per-vp command. Lower values from 0 to 31 are usually reserved for specific traffic such as: F4 Operation Administration and Maintenance (OAM), SSL VPN Client (SVC) signaling, Interim Local Management Interface (ILMI), and so on.; and should not be used. The VCI value is a 16-bit field in the header of the ATM cell. The VCI value is unique only on a single link, not throughout the ATM network, because it has local significance only. A value that is out of range causes an “unrecognized command” error message. The arguments vpi and vci cannot both be set to 0; if one is 0, the other cannot be 0.

Command Default No PVC is defined.

Command Modes

Interface configuration (config-if)
Subinterface configuration (config-subif)

Usage Guidelines

This command is used to create or assign a name to an ATM permanent virtual circuit (PVC), to specify the encapsulation type on an ATM PVC, and to enter ATM virtual circuit configuration mode.

When a PVC is defined, the global default of the encapsulation command applies (aal5snap). Use the **pvc** command to configure a single ATM VC only, not a VC that is a bundle member.

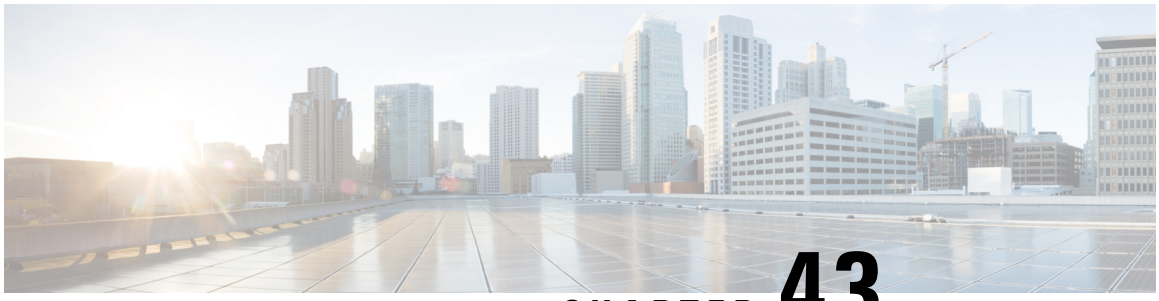
Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Examples

The following example specifies the output PCR for an ATM PVC to be 100,000 kbps, the output SCR to be 50,000 kbps, and the output MBS to be 64:

```
Device# config-t
Device(config)# interface ATM 0/2/0
Device(config-if)# no shut
Device(config-if)# interface ATM 0/2/0.1 point-to-point
Device(config-subif)# pvc 0/32
```



CHAPTER 43

PPPoEoVlan Commands

- class (class-map), on page 627
- dialer-group, on page 628
- dialer pool, on page 629
- encapsulation, on page 630
- interface Dialer, on page 631
- ip address, on page 631
- ip address negotiated, on page 632
- ip unnumbered, on page 633
- ppp authentication, on page 633
- ppp chap hostname, on page 634
- ppp chap password, on page 635
- ppp pap sent-username password, on page 636
- pppoe-client dial-pool-number, on page 637
- pppoe-client ppp-max-payload, on page 638
- pppoe enable group, on page 639
- protocol ppp dialer, on page 640
- set cos, on page 641

class (class-map)

To specify the name of the class whose policy you want to create or change before you configure its policy, use the **class**command in class-map configuration mode. To remove a class from the class map, use the **no** form of this command.

class *class-name*
no class { *class-name* }

Syntax Description

class-name	Name of the class to be configured or whose policy is to be modified. The class name is used for both the class map and to configure a policy for the class in the policy map.

Command Default

No class is specified.

Command Modes

Class-map configuration (config-class-map)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE, class command.

Examples

The following is an example of this command:

```
Device(config)# policy
Device(config-policy)# class-map
Device(config-class-map)# class VOICE queue 0
```

dialer-group

To control access by configuring an interface to a specific dialer group, use the **dialer-group** command in interface configuration mode. To remove an interface from the specified dialer access group, use the **no** form of this command

dialer-group *group-number*

no dialer-group *group-number*

Syntax Description

group-number	Number of the dialer access group to which the specific interface belongs. The range is from 1 to 128.

Command Default

None

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

An interface can be associated with a single dialer access group only. You cannot assign multiple dialer-groups. This command can be used to control access by configuring an interface to a specific dialer group.

Example

The following example shows how to configure Interface Dialer1 to Dialer-Group 1.

```
Device# config-transaction
Device(config)# interface Dialer1
Device(config-if)# dialer-group 1
```

Related Commands

Command	Description
interface dialer	Defines a dialer rotary group.
pppoe-client dial-pool-number	Configures the dialer pool to which the interface belongs.
dialer-list	Specifies an access list by list number or by protocol, and the list number defines the "interesting" packets that can trigger a call.

dialer pool

To specify, for a dialer interface, which dialing pool to use to connect to a specific destination subnetwork, use the **dialer pool** command in interface configuration mode. To remove the dialing pool assignment, use the **no** form of this command.

dialer pool *number*

no dialer pool

Syntax Description

number	Dialing pool number, in the range 1 through 255.

Command Default

Disabled; no default number is specified.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

This command applies to dialer interfaces only

Example

```
Device(config)# interface Dialer 1
Device(config-if)# dialer pool 1
```

encapsulation

To set the encapsulation method used by the interface, use the **encapsulation** command in interface configuration mode. To remove the encapsulation, use the **no** form of this command.

encapsulation *encapsulation-type*
no encapsulation *encapsulation-type*

Syntax Description

encapsulation-type	Encapsulation type; one of the following keywords: • **dot1q** *vlan-id* ---Enables IEEE 802.1q encapsulation of traffic on a specified subinterface in VLANs. The *vlan-id* argument is a virtual LAN identifier. • **frame-relay** --Frame Relay (for serial interface). • **ppp** -- PPP (for Dialer interface).

Command Default

NA

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates. The following keywords are qualified: • **dot1q** for GigabitEthernet interface . • **ppp** for Dialer interface.
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Command qualified for use in Cisco vManage CLI templates. The following keywords are qualified: • **encapsulation frame-relay** for serial interface.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE encapsulation command.

Examples

The following example shows how to enable frame-relay encapsulation on Serial interface 0:

```
Device(config)# interface Serial 0
Device(config-if)# encapsulation frame-relay
```

The following example shows how to configure Dialer interface 1 for PPP encapsulation:

```
Device(config)# interface Dialer 1
Device(config-if)# encapsulation ppp
```

interface Dialer

To define a dialer rotary group or profile, use the **interface Dialer** command in global configuration mode. To remove the configuration, use the **no** form of this command.

interface Dialer *dialer-rotary-group-number*

no Interface Dialer *dialer-rotary-group-number*

Syntax Description

dialer-rotary-group-number	Number of the dialer rotary group in the range from 0 to 255.

Command Default

No dialer rotary groups are predefined.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE interface Dialer command.

Examples

The following example identifies interface dialer 2 as the dialer rotary group leader. Interface dialer 2 is not a physical interface, but represents a group of interfaces.

```
Device(config)# interface Dialer 2
```

ip address

To set a primary or secondary IP address for an interface, use the **ip address** command in interface or sub-interface configuration mode. To remove an IP address or disable IP processing, use the **no** form of this command.

ip address *ip-address* [*mask*]
no ip address [*ip-address*] [*mask*]

Syntax Description

ip-address	IP address.
mask	(Optional) Mask for the associated IP subnet.

Command Default

No IP address is defined for the interface.

Command Modes

Interface configuration (config-if)

Sub-interface configuration (config-subif)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For the usage guidelines, see the Cisco IOS XE ip address command.

Examples

```
Device(config)# interface ATM 0/3/0.1 point-to-point
Device(config-if)# ip address 192.10.6.5
Device(config)# interface ATM 0/3/0.1
Device(config-subif)# ip address 10.0.0.0 255.255.255.252
Device(config)# interface Serial 0/1/0.2
Device(config-if)# ip address 10.1.1.1 255.255.255.0
Device(config)# interface Serial 0/0/1:5
Device(config-if)# ip address 10.1.1.1 255.255.255.0
Device(config)# interface MFR1
Device(config-if)# ip address 10.4.4.4 255.255.255.0
```

ip address negotiated

To configure an interface and to use the address that is obtained during IPCP negotiation, use **ip address negotiated** command in interface configuration mode. To remove the configuration, use the **no** form of this command.

ip address negotiated

no ip address negotiated

Syntax Description

This command has no keywords or arguments.

Command Default

By default, no ip address method is set.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

The IP Control Protocol (IPCP) is used for configuring, enabling, and disabling the IP protocol modules on both ends of the Point-to-Point (PPP) link.

This command can be used to configure an interface to use the address that is obtained during IPCP negotiation. This command is used under the Dialer interface command which is configured for PPP connections.

Example

The following example shows how to configure interface Dialer1 to use the address that is obtained during IPCP negotiation.

```
Device# config-transaction
Device(config)# interface Dialer1
Device(config-if)# ip address negotiated
```

Related Commands

Command	Description
interface dialer	Defines a dialer rotary group.

ip unnumbered

To enable IP processing on an interface without assigning an explicit IP address to the interface, use the **ip unnumbered** command in interface configuration mode or subinterface configuration mode. To disable the IP processing on the interface, use the **no** form of this command.

ip unnumbered *type*
no ip unnumbered

Syntax Description

type	Type of interface. For more information, use the question mark (**?**) online help function.

Command Default

Unnumbered interfaces are not supported.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE ip unnumbered command.

Examples

The following example shows how to configure GigabitEthernet 1 as an IP unnumbered interface.

```
Device(config)# interface Tunnel 1
Device(config-if)# ip unnumbered GigabitEthernet1
```

ppp authentication

To enable at least one PPP authentication protocol and to specify the order in which the protocols are selected on the interface, use the **ppp authentication** command in interface configuration mode. To disable this authentication, use the **no** form of this command.

ppp authentication *protocol1* [*protocol2*] [**callin**]

no ppp authentication *protocol1* [*protocol2*] [**callin**]

Syntax Description

protocol 1	One of the authentication methods is supported, in order of preference. Options are PAP or CHAP.
callin	(Optional) Authentication is on incoming (received) calls only.

Command Default

PPP authentication is not enabled.

Command Modes

Interface Configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

When you enable Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP), the local router requires the remote device to prove its identity before allowing data traffic to flow. PAP authentication requires the remote device to send a name and a password, which is checked against a matching entry in the local username database or in the remote security server database. CHAP authentication sends a challenge message to the remote device. The remote device encrypts the challenge value with a shared secret and returns the encrypted value and its name to the local router in a Response message. The local router attempts to match the name of the remote device with an associated secret stored in the local username or remote security server database; it uses the stored secret to encrypt the original challenge and verify that the encrypted values match.

In order to configure PPP Authentication, you must configure the encapsulation of the interface as PPP.

Example

The following example shows how to configure CHAP authentication on interface Dialer1.

```
Device# config-transaction
Device(config)# interface Dialer1
Device(config-if)# encapsulation ppp
Device(config-if)# ppp authentication chap
```

Related Commands

Command	Description
encapsulation ppp	Configures the PPP as the encapsulation protocol for an interface.

ppp chap hostname

To create a pool of dialup routers by specifying a common alias for all routers when authenticating with CHAP (Challenge Handshake Authentication Protocol), use the **ppp chaphostname** command in interface configuration mode. To disable this function, use the no form of the command.

ppp chap hostname *hostname*
no ppp chap hostname

Syntax Description

hostname	The name sent in the CHAP challenge.

Command Default Disabled. The router name is sent in any CHAP challenges.

Command Modes Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines The command is available only when **encapsulation ppp** is configured.

The **ppp chap hostname** command allows you to specify a common alias for all routers in a rotary group to use so that only one username must be configured on the dialing routers.

This command is normally used with local CHAP authentication (when the router authenticates to the peer), but it can also be used for remote CHAP authentication.

Note By default, after changing hostnames, an MLP member link does not undergo failure recovery automatically. You must use the **ppp chap hostname** command to define the Multilink PPP (MLP) bundle name on an endpoint. If this command is not configured and the hostname is changed, then a link flap will not return the link back to the bundle.

Examples

```
Device(config)# interface Dialer 1
Device(config-if)# encapsulation ppp
Device(config-if)# ppp chap hostname ntt
```

ppp chap password

To configure a common CHAP secret to be used in responses to challenges from an unknown remote peer in a collection of routers that do not support this command (such as routers running older Cisco IOS software images), use the **ppp chap password** interface configuration command. To disable this function, use the **no** form of this command.

ppp chap password *secret*
no ppp chap password *secret*

Syntax Description

secret	The secret used to compute the response value for any CHAP challenge from an unknown peer.

Command Default Disabled

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

The command is available only when **encapsulation ppp** is configured.

This command allows you to replace several username and password configuration commands with a single copy of this command on any dialer interface or asynchronous group interface.

This command is used for remote CHAP authentication only (when routers authenticate to the peer) and does not affect local CHAP authentication.

Examples

```
Device(config)# interface Dialer 1
Device(config-if)# encapsulation ppp
Device(config-if)# ppp chap password ntt
```

ppp pap sent-username password

To enable remote Password Authentication Protocol (PAP) support for an interface, and to use the values specified for username and password in the PAP authentication request, use the **ppp pap sent-username password** command in interface configuration mode. To disable remote PAP support, use the **no** form of this command.

ppp pap sent-username *username* **password** *password*

no ppp pap sent-username *username*

Syntax Description

username	Username sent in the PAP authentication request.
password	Cleartext or already-encrypted password.

Command Default

Remote PAP support is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

Use the **ppp pap sent-username password** command to enable remote PAP support (for example, to respond to the peer's request to authenticate with PAP) and to specify the parameters to be used when sending the PAP authentication request.

You must configure the **ppp pap sent-username password** command for each interface.

The command is available only when **virtual-ppp** is configured.

Examples

In the following example, a password is entered as a cleartext password, xxxx for remote PAP authentication:

```
router# configure
router(config)# interface POS 0/1/0/0
router(config-if)# ppp pap sent-username xxxx password notified
router(config-if)# ppp pap sent-username xxxx password clear notified
```

pppoe-client dial-pool-number

To configure a PPP over Ethernet (PPPoE) client, use the **pppoe-client dial-pool-number** command in interface configuration mode or VLAN interface configuration mode. To disable the configured dial-on-demand functionality, use the **no** form of this command.

pppoe-client dial-pool-number *number* [**service-name** *name*]
no pppoe-client dial-pool-number [*number*] [**service-name**]

Syntax Description

number	A number that is assigned to a configured dialer pool. The range is from 1 to 255.
service-name *name*	(Optional) Specifies the service name requested by the PPPoE client. • The service name that allows the PPPoE client to signal a service name to the Broadband Access Aggregation System (BRAS). • By default, no service name is signaled and the service name value is set to NULL.

Command Default

A PPPoE client is not configured and the DDR functionality is disabled.

Command Modes

Interface configuration (config-if)

VLAN interface configuration (config-VLAN-*vlan-id*)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Command qualified for use in Cisco vManage CLI templates. The following optional parameter is qualified: **service-name** *name*

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `pppoe-client dial-pool-number` command.

Examples

The following example shows PPPoE client configuration for a VLAN interface:

```
Device(config)# interface Vlan 1
Device(config-Vlan-1)# pppoe-client dial-pool-number 1
```

The following example shows PPPoE client configuration for a GigabitEthernet interface:

```
Device(config)# interface GigabitEthernet 4.302
Device(config-Vlan-1)# pppoe-client dial-pool-number 1 service-name ser1
```

pppoe-client ppp-max-payload

To set a Maximum Receive Unit (MRU) value to be negotiated during PPP Link Control Protocol (LCP) negotiation on an interface, use the **pppoe-client ppp-max-payload** command in interface configuration mode. To remove the MRU value, use the **no** form of this command.

pppoe-client ppp-max-payload *size*

no pppoe-client ppp-max-payload *size*

Syntax Description

size	Enter the Maximum Receive Unit (MRU) value to be negotiated during PPP LCP negotiation. Range is from 64 to 1792 bytes.

Command Default

By default, the MRU value to be negotiated during PPP LCP negotiation is 1492 bytes.

Command Modes

Interface configuration (config-if).

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

A PPPoE client and a server negotiate different parameters during the during PPP LCP phase, including the MTU and MRU of the interface.

This command can be used to set MRU size for a specific interface for the LCP negotiation.

In order to configure **pppoe-client ppp-max-payload** command, you must first configure the **pppoe-client dial-pool-number** command.

Example

The following example shows how to set the MRU to 1492 bytes on Interface GigabitEthernet 0/0/1:

```
Device# config-transaction
Device(config)# interface GigabitEthernet 0/0/1
Device(config-if)# pppoe-client dial-pool-number 1
Device(config-if)# pppoe-client ppp-max-payload 1492
```

Related Commands

Command	Description
pppoe-client dial-pool-number	Configures the dialer pool to which the interface belongs.

pppoe enable group

To enable a PPPoE session on the Gigabit Ethernet interface or subinterface, use the **pppoe enable group** command in interface configuration mode. To disable a PPPoE session, use the **no** form of this command.

pppoe enable [**group** { *profile-name* | **global** }]

no pppoe enable [**group** { *profile-name* | **global** }]

Syntax Description

profile-name	PPPoE profile name.
global	If a PPPoE profile is not assigned to the interface by using the group group-name option, the interface will use the global PPPoE profile.

Command Default

None

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

This command is used to enable a PPPoE session on the Gigabit Ethernet interface or or subinterface. If a PPPoE profile is not assigned to the interface by using the **group** *profile-name* option, the interface will use the global PPPoE profile.

Example

The following example shows how to enable a PPPoE session on the Gigabit Ethernet subinterface GigabitEthernet0/0/1.101.

```
Device# config-t
Device(config)# interface GigabitEthernet0/0/1.101
Device(config-if)# ip address 192.10.6.5 255.255.255.0
Device(config-if)# encapsulation dot1Q 101
Device(config-if)# pppoe enable group global
Device(config-if)# pppoe-client dial-pool-number 1
```

Related Commands

Command	Description
pppoe client dial pool-number	Configures a PPPoE client and specifies Dial-on-Demand Routing (DDR) functionality.

protocol ppp dialer

To configure a static map for an Asynchronous Transfer Mode (ATM) Permanent Virtual Circuit (PVC), use the **protocol ppp dialer** command in the interface ATM virtual circuit configuration mode. To remove the static mapping, use the **no** form of this command.

protocol ppp dialer

no protocol ppp dialer

Syntax Description

This command has no keywords or arguments.

Command Default

No default behaviour or value

Command Modes

Interface ATM virtual circuit configuration (config-if-pvc)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

This command is used to configure a static map for an ATM PVC, Switched Virtual Circuit (SVC), or Virtual Circuit (VC) class.

Example

The following example shows how to configure PPPoA on an ATM interface with a Point-to-Point subinterface using PVC 0/100.

```
Device# config-transaction
Device(config)# interface ATM 0/3/0
Device(config-if)# no shutdown
Device(config-if)# ip mtu 1496
Device(config-if)# interface ATM 0/3/0.1 point-to-point
Device(config-subif)# ip mtu 1496
Device(config-subif)# ip address 10.0.0.0 255.255.255.252
Device(config-subif)# no shutdown
Device(config-subif)# pvc 0/100
Device(config-if-pvc)# dialer pool-member 1
Device(config-if-pvc)# protocol ppp dialer
```

Related Commands

Command	Description
pvc	Specifies the encapsulation type on an ATM PVC and enters config-if-pvc mode.
dialer pool-member	Configures a physical interface to be a member of a dialer profiles dialing pool.

set cos

To set the Layer 2 class of service (CoS) value of an outgoing packet, use the **setcos** command in policy-map class configuration mode. To remove a specific CoS value setting, use the **no** form of this command.

set cos *cos-value*
no set cos

Syntax Description

cos-value	Specific IEEE 802.1Q CoS value from 0 to 7.

Command Default

No CoS value is set for the outgoing packet.

Command Modes

Policy-map class configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

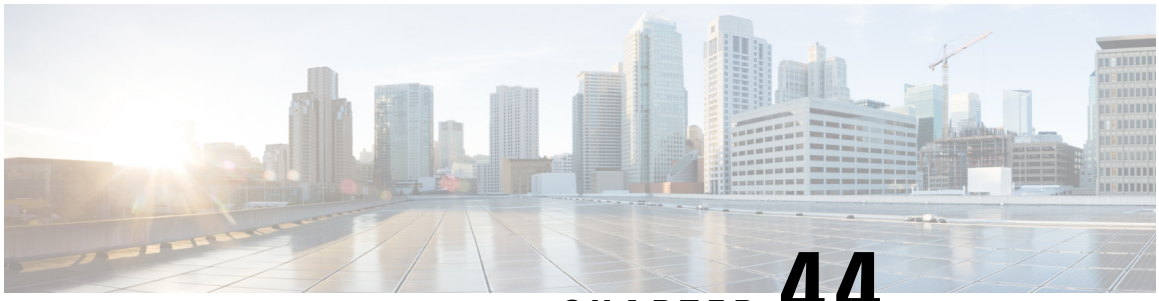
For usage guidelines, see the Cisco IOS XE `set cos` command.

Examples

In the following example, the policy map called “cos-set” is created to assign different CoS values for different types of traffic. This example assumes that the class maps called “voice” and “video-data” have already been created.

```
Router(config)# policy-map cos-set
Router(config-pmap)# class voice
Router(config-pmap-c)# set cos 1
Router(config-pmap-c)# exit


Router(config-pmap)# class video-data
Router(config-pmap-c)# set cos 2
Router(config-pmap-c)# end
```



CHAPTER 44

QoS Policy Commands

- bandwidth, on page 643
- bandwidth (policy-map class), on page 644
- bandwidth qos-reference, on page 645
- bandwidth remaining ratio, on page 645
- class (policy-map), on page 646
- control-plane, on page 647
- ip nbar protocol-discovery, on page 648
- match access-group, on page 649
- match packet-tag, on page 649
- platform qos sdwan max-session, on page 650
- police (percent), on page 651
- policy-map, on page 652
- priority, on page 653
- priority level, on page 654
- random-detect, on page 655
- service-policy, on page 655
- service-policy (policy-map class), on page 656
- shape (policy-map class), on page 657
- vpn packet-tag, on page 657
- platform qos port-channel-aggregate, on page 658

bandwidth

To define the total bandwidth for a bandwidth pool, use the **bandwidth** command in bandwidth pool configuration mode. To return to the default value, use the **no** form of this command.

Supported Parameters

value	Specifies the total bandwidth, in kilobits per second, for a bandwidth pool. Valid value is a number from 1 to 4294967295.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE bandwidth command.

Examples

```
interface serial 0
bandwidth 44736
```

bandwidth (policy-map class)

To specify or modify the bandwidth allocated for a class belonging to a policy map, or to enable ATM overhead accounting, use the **bandwidth** command in QoS policy-map class configuration mode. To remove the bandwidth specified for a class or disable ATM overhead accounting, use the **no** form of this command.

bandwidth [**remaining**] **percent** *percentage*
no bandwidth

Syntax Description

remaining	(Optional) Specifies that the percentage of guaranteed bandwidth is based on a relative percent of available bandwidth.
percent *percentage*	Specifies the percentage of guaranteed bandwidth based on an absolute percent of available bandwidth to be set aside for the priority class or on a relative percent of available bandwidth. The valid range is 1 to 100.

Command Default

No bandwidth is specified.

Command Modes

QoS policy-map class configuration (config-pmap-c)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

For usage guidelines, see the Cisco IOS XE `bandwidth (policy-map class)` command.

Examples

The following example shows how to create two policy maps called “PMap” and "generic-cos" and configure two class policies in each policy map.

```
policy-map PMap
 class PMap-super-fast
  priority level 1
  police percent 5
 !
 class PMap-fast
  priority level 2
  police percent 5
```

```
 !
!
policy-map generic-cos
 class cos-map-generic
  bandwidth remaining percent 5
  queue-limit 108 packets
 !
 class class-default
  bandwidth remaining percent 95
  queue-limit 2028 packets
 !
!
```

bandwidth qos-reference

To configure bandwidth to be used as a reference for calculating rates of quality of service (QoS) percent configurations on a physical or logical interface, use the **bandwidthqos-reference** command in interface configuration or subinterface configuration mode. To remove this explicitly specified reference bandwidth, use the **no** form of this command.

bandwidth qos-reference *bandwidth-amount*
no bandwidth qos-reference *bandwidth-amount*

Syntax Description

bandwidth-amount	Amount of bandwidth in kilobits per second (kb/s). Valid values are 1 to 10000000.

Command Default

This command is disabled. Reference bandwidth for a logical interface is derived from the main interface or the main interface QoS policy.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For the usage guidelines, see bandwidth qos-reference.

Examples

The following example shows how to configure the **bandwidthqos-reference** command to allocate 100000 kb/s of bandwidth as a reference rate for GigabitEthernet interface 1:

```
Device(config)# interface GigabitEthernet 1
Device(config-if)# bandwidth qos-reference 100000
```

bandwidth remaining ratio

To specify a bandwidth-remaining ratio for class-level or subinterface-level queues to be used during congestion to determine the amount of excess bandwidth (unused by priority traffic) to allocate to nonpriority queues,

use the **bandwidth remaining ratio** command in policy-map class configuration mode. To remove the bandwidth remaining ratio, use the **no** form of this command.

bandwidth remaining ratio *ratio*
no bandwidth remaining ratio *ratio*

Syntax Description

ratio	Relative weight of this subinterface or class queue with respect to other subinterfaces or class queues. Valid values are from 1 to 1000. At the subinterface level, the default value is platform dependent. At the class queue level, the default is 1.
ratio	Relative weight of this subinterface or class queue with respect to other subinterfaces or class queues.

Command Default

The default bandwidth ratio is 1.

Command Modes

Policy-map class (config-pmap-c)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `bandwidth remaining ratio` command.

Examples

```
class Queue1
   bandwidth remaining ratio 20
   random-detect precedence-based
  !
```

class (policy-map)

To specify the name of the class whose policy you want to create or change or to specify the default class (commonly known as the class-default class) before you configure its policy, use the **class**command in policy-map configuration mode. To remove a class from the policy map, use the **no** form of this command.

class { *class-name* | **class-default** }
no class { *class-name* | **class-default** }

Syntax Description

class-name	Name of the class to be configured or whose policy is to be modified. The class name is used for both the class map and to configure a policy for the class in the policy map.
class-default	Specifies the default class so that you can configure or modify its policy.

Command Default

No class is specified.

Command Modes

Policy-map configuration (config-pmap)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `class (policy-map)` command.

Examples

The following example shows how to create two policy maps called “PMap” and "generic-cos" and configure two class policies in each policy map.

```
policy-map PMap
 class PMap-super-fast
  priority level 1
  police percent 5
 !
 class PMap-fast
  priority level 2
  police percent 5
 !
!
policy-map generic-cos
 class cos-map-generic
  bandwidth remaining percent 5
  queue-limit 108 packets
 !
 class class-default
  bandwidth remaining percent 95
  queue-limit 2028 packets
 !
!
```

control-plane

To configure a quality of service (QoS) filter that manages the traffic flow of control plane packets to protect the control plane of Cisco IOS XE routers and switches against reconnaissance and denial-of-service (DoS) attacks, use the **control-plane** command in the appropriate configuration mode. To remove the control plane from an input or output interface, use the **no** form of this command.

control-plane service-policy **input** *policy-map-name* **output** *policy-map-name*
no **control-plane service-policy**

Syntax Description

service-policy	Attaches a QoS service policy to the control plane.
input	Applies the specified service policy to packets received on the control plane.
output	Applies the specified service policy to packets transmitted from the control plane and enables the router to silently discard packets..
policy-map-name	The name of a service policy map (created using the **policy-map** command) to be attached. The name can be a maximum of 40 alphanumeric characters in length.

Command Default No control policy is specified. No policy map is attached.

Command Modes Interface configuration (config-if)

Subinterface configuration (config-subif)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	Qualified for use in Cisco Catalyst SD-WAN Manager CLI templates.

Usage Guidelines For the usage guidelines, see control-plane.

Examples

```
Device(config)# interface GigabitEthernet 1
Device(config-if)# control-plane input policy_1
```

Examples

```
Device(config)# interface GigabitEthernet 1
Device(config-if)# control-plane output policy_2
```

ip nbar protocol-discovery

To configure Network-Based Application Recognition (NBAR) to discover traffic for all protocols that are known to NBAR on a particular interface, use the **ipnbarprotocol-discovery** command in interface configuration mode or VLAN configuration mode. To disable traffic discovery, use the **no** form of this command.

ip nbar protocol-discovery
no ip nbar protocol-discovery

Syntax Description This command has no arguments or keywords.

Command Default Traffic discovery is disabled.

Command Modes Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release Amsterdam 17.2.1v	Qualified for use in Cisco vManage CLI templates

Usage Guidelines For the usage guidelines, see ip nbar protocol-discovery.

Examples The following example shows how to configure protocol discovery for both IPv4 and IPv6 on an Ethernet interface:

```
Device(config)# interface GigabitEthernet 1.101
Device(config-if)# ip nbar protocol-discovery
```

match access-group

To configure the match criteria for a class map on the basis of the specified access control list (ACL), use the **match access-group** command in class-map configuration mode. To remove ACL match criteria from a class map, use the **no** form of this command.

match access-group name *access-group-name*
no match access-group name *access-group-name*

Syntax Description

name *access-group-name*	Named ACL whose contents are used as the match criteria against which packets are checked to determine if they belong to this class. The name can be a maximum of 40 alphanumeric characters.

Command Default

No match criterion is specified.

Command Modes

QoS class-map configuration (config-cmap)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Examples

```
class-map type inspect match-all cmap
  match access-group name cmap
 !
```

match packet-tag

To configure the match criteria for a class map on the basis of the packet-tag type, value, and mask use the **match packet-tag** command in the class-map configuration mode. To remove the match criteria, use the **no** form of the command.

match packet-tag *type value mask*

Syntax Description

type	The packet-tag type is a value in the range 1 to 8. For VPN traffic, the packet-tag type is configured using the **vpn packet-tag** command.
value	For VPN traffic, the packet-tag value is the VPN ID.
mask	The mask is used to identify a single VPN ID, or a VPN ID from a range of IDs. For a single VPN ID, use the mask 65535. To identify a VPN ID from a range of IDs, calculate the mask such that an AND operation between the VPN ID and the mask evaluates to the first VPN ID in the range.

Command Default By default, the command is not configured.

Command Modes QoS class-map configuration (config-cmap)

Command History

Release	Modification
Cisco IOS XE Release 17.6.1a	Command introduced.

Example

In the following example, match criteria is specified for a sequence of VPN IDs that do not belong to a range:

```
class-map match-any VPN_GROUP_1
 match packet-tag 1 101 65535
 match packet-tag 1 201 65535
```

In the following example, match criteria is specified for a sequence of VPN IDs that belong to a range:

```
class-map match-any VPN_GROUP_103
 match packet-tag 1 103 65535
 match packet-tag 1 104 65534
```

platform qos sdwan max-session

To configure the maximum number of sessions to which a QoS policy can be applied, use the **platform qos sdwan max-session** command in global configuration mode. To restore the maximum number of sessions to the default, use the **no** form of the command.

platform qos sdwan max-session *number-of-sessions* [**adapt** { **mode** { **aggressive** | **normal** } [**spoke-overlay-usage** *usage-percent*] [**wan-loss-permillage** *permillage*] }]

no platform qos sdwan max-session

Syntax Description

number-of-sessions	Number of sessions to which a QoS policy can be applied, set individually for each tunnel. Range (Cisco IOS XE Catalyst SD-WAN Release 17.13.1a): 100 through 10,000 Range (Cisco IOS XE Catalyst SD-WAN Release 17.11.1a): 100 through 6,000
adapt	This is the first phase where the shaping rate (the mechanism that regulates the data transfer rate in a network) is determined either by the default value or recalculated based on the results from the previous cycle.

mode	Adjust the shaping rate based on the current throughput or the existing shaping rate. The shaping rate is the maximum data transfer rate that a network traffic shaper allows on a network link. **aggressive**: Use the current throughput. **normal**: Use the current shaping rate.
spoke-overlay-usage *usage-percent*	The percentage of spoke-overlay-usage. This is the proportion of the total network capacity for spoke connections in the network's overlay architecture. Range: 1 through 100 percent
wan-loss-permillage *permillage*	WAN loss permillage is the packet loss rate on the WAN link, in parts per thousand (per mille). Range: 1 through 999

Command Default

The default maximum number of QoS sessions is dependent on the platform.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	Command qualified for use in Cisco Catalyst SD-WAN Manager CLI templates.
Cisco IOS XE Catalyst SD-WAN Release 17.13.1a	Increased the maximum number of sessions from 6,000 to 10,000.

Usage Guidelines

Use the **platform qos sdwan max-session** command to configure the maximum number of sessions to which a QoS policy can be applied, on a per-tunnel basis. When the Cisco Catalyst SD-WAN Manager user sessions with QoS policy reach the limit, QoS policy is not applied for additional sessions.

Configure Maximum Number of Sessions

The following example shows how configure the per-tunnel QoS scale to support up to 10,000 sessions.

```
Device(config)# platform qos sdwan max-session 10000
```

police (percent)

To configure traffic policing on the basis of a percentage of bandwidth available on an interface, use the **police** command in policy-map class configuration mode. To remove traffic policing from the configuration, use the **no** form of this command.

police rate percent *percentage*
no police rate percent *percentage*

Syntax Description

rate	Specifies the information rate.

percent	Specifies that a percentage of bandwidth will be used for calculating the CIR.
percentage	The bandwidth percentage. Valid range is a number from 1 to 100.

Command Default

No traffic policing is configured.

Command Modes

Policy-map class configuration (config-pmap-c)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `police (percent)` command.

Examples

The following example shows how to configure traffic policing:

```
Policy-map PMap
 class PMap-super-fast
  priority level 1
  police rate percent 5
 class PMap-fast
  priority level 2
  police rate percent 5
 !
!
policy-map generic-cos
 class cos-map-generic
  bandwidth remaining percent 5
  queue-limit 108 packets
 class class-default
  bandwidth remaining percent 95
  queue-limit 2028 packets
```

policy-map

To enter policy-map configuration mode and create or modify a policy map that can be attached to one or more interfaces to specify a service policy, use the **policy-map**command in global configuration mode. To delete a policy map, use the **no** form of this command.

policy-map [**type inspect**] *policy-map-name*
no policy-map [**type inspect**] *policy-map-name*

Syntax Description

type inspect	(Optional) Specifies the policy-map type as inspect.
policy-map-name	Name of the policy map.

Command Default

The policy map is not configured.

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Qualified for use in Cisco vManage CLI templates.
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	Command modified to support **type inspect**.

Usage Guidelines For usage guidelines, see the Cisco IOS XE `policy-map` command.

Examples

The following example shows how to create two policy maps called “PMap” and "generic-cos" and configure two class policies in each policy map.

```
policy-map PMap
 class PMap-super-fast
  priority level 1
  police percent 5
 !
 class PMap-fast
  priority level 2
  police percent 5
 !
!
policy-map generic-cos
 class cos-map-generic
  bandwidth remaining percent 5
  queue-limit 108 packets
 !
 class class-default
  bandwidth remaining percent 95
  queue-limit 2028 packets
 !
!
```

priority

To give 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 percent *percentage*
no priority percent *percentage*

Syntax Description

percent	Specifies that the amount of guaranteed bandwidth will be specified by the percent of available bandwidth.
percentage	Total available bandwidth to be set aside for the priority class. The percentage can be a number from 1 to 100.

Command Default No priority is set.

Command Modes

Policy-map class configuration (config-pmap-c)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `priority` command

Examples

```
policy-map QOS-POLICY-MAP
 class Queue0
  priority percent 30
 class Queue1
  bandwidth percent 20
 class Queue3
  bandwidth percent 20
 class class-default
  bandwidth percent 30
```

priority level

To configure multiple priority queues, use the **priority level** command in policy-map class configuration mode. To remove a previously specified priority level for a class, use the **no** form of this command.

priority level *level*
no priority level *level*

Syntax Description

level	Defines multiple levels of a strict priority service model. When you enable a traffic class with a specific level of priority service, the implication is a single priority queue associated with all traffic that is enabled with the specified level of priority service. Valid values are from 1 (high priority) to 2 (low priority). Default is 1.

Command Default

The priority level has a default level of 1.

Command Modes

Policy-map class configuration (config-pmap-c)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `priority level` command.

Examples

The following example shows how to configure multi level priority queues. In the example, the traffic class named PMap-super-fast is given high priority (level 1), and the class named PMap-fast is given

level 2 priority. To prevent PMap-fast traffic from becoming starved of bandwidth, PMap-super-fast traffic is policed at 5 percent of the available bandwidth.

```
Policy-map PMap
 class PMap-super-fast
  priority level 1
  police percent 5
 class PMap-fast
  priority level 2
  police percent 5
 !
!
```

random-detect

random-detect
no random-detect

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 Catalyst SD-WAN Release 17.2.1r	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `random-detect` command

Examples

```
policy-map policy1
 class class1
 bandwidth percent 80
 random-detect
```

service-policy

To attach a policy map to an input interface or an output interface, use the **service-policy** command in the appropriate configuration mode. To remove a service policy from an input or output interface, use the **no** form of this command.

service-policy output *policy-map-name*
no service-policy

Syntax Description

output	Attaches the specified policy map to the output interface or output VC.
policy-map-name	The name of a service policy map (created using the **policy-map** command) to be attached. The name can be a maximum of 40 alphanumeric characters in length.

Command Default

No service policy is specified. A control policy is not applied to a context. No policy map is attached.

Command Modes

Interface configuration (config-if)

Subinterface configuration (config-subif)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For the usage guidelines, see service-policy.

Examples

```
Device(config)# interface GigabitEthernet 1
Device(config-if)# service-policy output  policy_1
```

Examples

```
Device(config)# interface ATM 0/2/0.1 point-to-point
Device(config-subif)# service-policy output  policy_1
```

service-policy (policy-map class)

To use a service policy as a QoS policy within a policy map (called a hierarchical service policy), use the **service-policy** command in policy-map class configuration mode. To disable a particular service policy as a QoS policy within a policy map, use the **no** form of this command.

service-policy *policy-map-name*
no service-policy *policy-map-name*

Syntax Description

policy-map-name	Specifies the name of the predefined policy map to be used as a QoS policy. The name can be a maximum of 40 alphanumeric characters.

Command Default

No service policies are used.

Command Modes

Policy-map class configuration (config-pmap-c)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `service-policy (policy-map class)` command.

Examples

The following example creates a hierarchical service policy in the service policy called parent:

```
policy-map shape_GigabitEthernet0/0/1
 class class-default
  service-policy Branch-QoS-Policy
  shape average 1000000000
```

shape (policy-map class)

To shape traffic to the indicated bit rate according to the algorithm specified or to enable ATM overhead accounting, use the **shape** command in policy-map class configuration mode. To remove shaping and leave the traffic unshaped, use the **no**form of this command.

shape average *mean-rate*
no shape [**average**]

Syntax Description

average	Committed Burst (Bc) is the maximum number of bits sent out in each interval.
mean-rate	Also called committed information rate (CIR). Indicates the bit rate used to shape the traffic, in bps. When this command is used with backward explicit congestion notification (BECN) approximation, the bit rate is the upper bound of the range of bit rates that will be permitted. The value must be between 1,000 and 1,000,000,000 bits per second.

Command Default

Command Modes

Policy-map class configuration (config-pmap-c)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `shape (policy-map class)` command.

Examples

```
policy-map shape_GigabitEthernet0/0/1
  class class-default
   service-policy Branch-QoS-Policy
   shape average 1000000000
  !
```

vpn packet-tag

To specify a packet-tag type for VPN traffic from the branch, use the **vpn packet-tag** command in the SD-WAN configuration mode. To remove the packet-tag type configuration, use the **no** form of the command.

vpn packet-tag *type*

no vpn packet-tag

Syntax Description

type	VPN packets are tagged with the specified type. On the physical interface, VPN packets are found using the tag type to apply per-VPN QoS. Specify a value in the range 1 to 8.

Command Default

By default, the command is disabled

Command Modes

sdwan configuration mode (config-sdwan)

Command History

Release	Modification
Cisco IOS XE Release 17.6.1a	Command introduced

Example

In the following example, VPN packets are tagged to be of type '1'.

```
sdwan
 vpn packet-tag 1
```

platform qos port-channel-aggregate

To enable the aggregate port-channel interface, use the **platform qos port-channel-aggregate** command in the global configuration mode.

platform qos port-channel-aggregate *port-channel-number*

no platform qos port-channel-aggregate *port-channel-number*

Syntax Description

port-channel-number	Specify an EtherChannel number.

Command Modes

Global configuration (config)

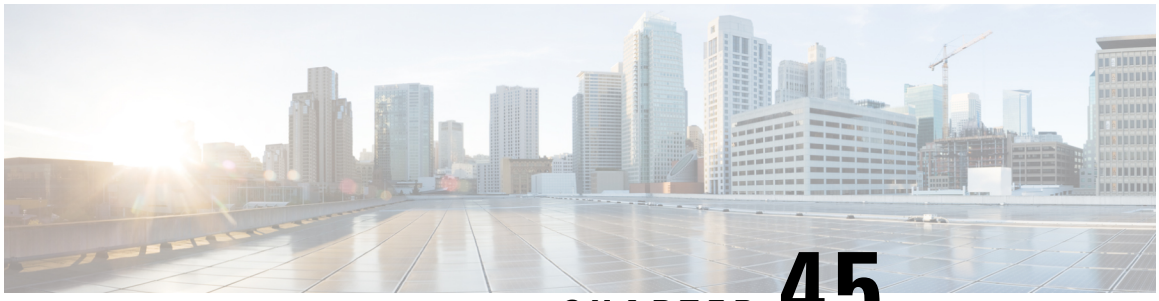
Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.13.1a	Command qualified for use in Cisco Catalyst SD-WAN Manager CLI templates.

Enable the aggregate port-channel interface

The following example shows how to enable the aggregate port-channel interface.

```
Device# config-transaction
Device(config)# platform qos port-channel-aggregate port-channel-number
```



CHAPTER 45

Radius Commands

Instructions for Radius Commands

Note Some configurations and protocols are identified as insecure and is a security risk for Cisco devices. Existing deployments continue to function, but new installations require intentional enablement. For more information on remediation, refer to Resilient Infrastructure: Cisco Catalyst SD-WAN and Routing

- radius-server dead-criteria, on page 659
- radius-server deadtime, on page 660

radius-server dead-criteria

To force one or both of the criteria--used to mark a RADIUS server as dead--to be the indicated constant, use the **radius-server dead-criteria** command in global configuration mode. To disable the criteria that were set, use the **no** form of this command.

radius-server dead-criteria [**time** *seconds*] [**tries** *number-of-tries*]

no radius-server dead-criteria [**time** *seconds*] [**tries** *number-of-tries*]

Syntax Description

time *seconds*	(Optional) Minimum amount of time, in seconds, that must elapse from the time that the router last received a valid packet from the RADIUS server to the time the server is marked as dead. If a packet has not been received since the router booted, and there is a timeout, the time criterion will be treated as though it has been met. You can configure the time to be from 1 through 120 seconds. • If the *seconds* argument is not configured, the number of seconds will range from 10 to 60 seconds, depending on the transaction rate of the server. **Note** Both the time criterion and the tries criterion must be met for the server to be marked as dead.

tries *number-of-tries*	(Optional) Number of consecutive timeouts that must occur on the router before the RADIUS server is marked as dead. If the server performs both authentication and accounting, both types of packets will be included in the number. Improperly constructed packets will be counted as though they were timeouts. All transmissions, including the initial transmit and all retransmits, will be counted. You can configure the number of timeouts to be from 1 through 100. • If the *number-of-tries* argument is not configured, the number of consecutive timeouts will range from 10 to 100, depending on the transaction rate of the server and the number of configured retransmissions. **Note** Both the time criterion and the tries criterion must be met for the server to be marked as dead.

Command Default

The number of seconds and number of consecutive timeouts that occur before the RADIUS server is marked as dead will vary, depending on the transaction rate of the server and the number of configured retransmissions.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For the usage guideline, see radius-server dead-criteria

Examples

```
Device (config)# radius-server dead-criteria time 5 tries 4
```

radius-server deadtime

To improve RADIUS response time when some servers might be unavailable and to skip unavailable servers immediately, use the **radius-server deadtime** command in global configuration mode. To set deadtime to 0, use the **no** form of this command.

radius-server deadtime *minutes*
no radius-server deadtime

Syntax Description

minutes	Length of time, in minutes (up to a maximum of 1440 minutes or 24 hours), for which a RADIUS server is skipped over by transaction requests.

Command Default

Dead time is set to 0.

Command Modes

Global configuration (config)

Command History

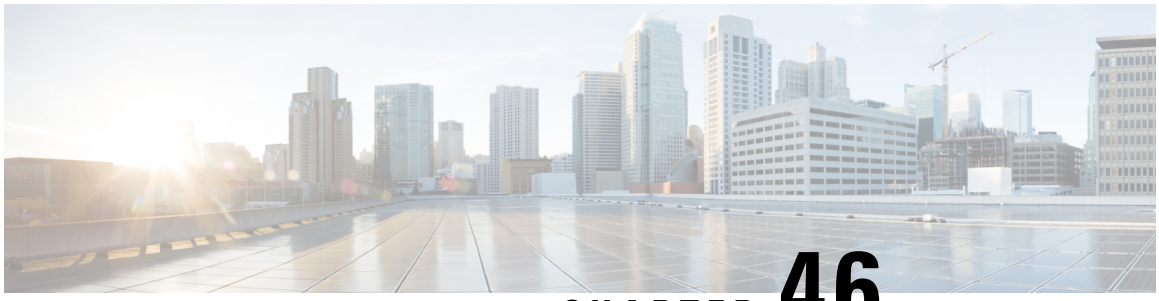
Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For the usage guideline, see radius-server deadtime

Examples

```
Device (config)# radius-server deadtime 5
```



CHAPTER 46

RIP Commands

- address-family ipv4 vrf, on page 664
- address-family ipv6, on page 664
- auto-summary (RIP), on page 665
- default-information originate (RIP), on page 666
- default-metric (RIP), on page 666
- distance (IP), on page 667
- distribute-list (RIP), on page 669
- distribute-list prefix-list (IPv6 RIP), on page 670
- input-queue, on page 671
- ip rip advertise, on page 671
- ip rip receive version, on page 672
- ip rip send version, on page 673
- ipv6 prefix-list, on page 674
- ipv6 rip default-information, on page 675
- ipv6 rip enable, on page 676
- ipv6 rip metric-offset, on page 677
- ipv6 rip summary-address, on page 677
- ipv6 rip vrf-mode enable, on page 678
- ipv6 router rip, on page 679
- ipv6 unicast-routing, on page 680
- maximum-paths, on page 680
- neighbor (RIP), on page 681
- network (RIP), on page 682
- offset-list (RIP), on page 683
- omp-route-tag, on page 684
- output-delay, on page 685
- passive-interface, on page 685
- redistribute, on page 686
- redistribute (IPv6), on page 687
- router rip, on page 688
- timers basic (RIP), on page 689
- traffic-share min, on page 690
- validate-update-source, on page 691

• version (RIP), on page 692

address-family ipv4 vrf

To enable Routing Information Protocol (RIP) under a Virtual Routing and Forwarding (VRF), use the **address-family ipv4 vrf** command in router configuration mode. To remove the address family from the RIP configuration, use the **no** form of this command.

address-family ipv4 [**unicast** | **vrf** *vrf-name*]
no address-family ipv4 [**unicast** | **vrf** *vrf-name*]

Syntax Description

ipv4	Selects the IPv4 protocol address family.
unicast	(Optional) Specifies the unicast address family.
vrf *vrf-name*	(Optional) Specifies the name of the VRF. This keyword/argument pair is required for RIP configurations.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE address-family ipv4 command.

Examples

The following example shows how to configure an IPv4 address family session for a VRF named 100:

```
vrf definition 100
  !
  rd 1:1
  address-family ipv4
   exit address-family
  !
router rip
  address-family ipv4 vrf 100
```

address-family ipv6

To enter address family configuration mode for configuring routing sessions, such as Routing Information Protocol (RIP), that use standard IPv6 address prefixes, use the **address-family ipv6** command in router configuration mode. To disable address family configuration mode, use the **no** form of this command.

address-family ipv6 vrf *vrf-name*
no address-family ipv6 vrf *vrf-name*

Syntax Description

vrf	Specifies VPN routing and forwarding (VRF) instance tables.

vrf-name	A specific VRF table for an IPv6 address.

Command Default

IPv6 address prefixes are not enabled.

Command Modes

Router configuration (config-rtr)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE address-family ipv6 command.

Examples

The following example shows how to place the router in address family configuration mode:

```
Device(config)# ipv6 router rip sdwan
Device(config-rtr)# address-family ipv6 vrf 1
Device(config-ipv6-router-af)# no address-family
Device(config-rtr)#
```

auto-summary (RIP)

To restore the default behavior of automatic summarization of subnet routes into network-level routes, use the **auto-summary** command in router configuration mode. To disable this function 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

When auto-summary is enabled, the software summarizes subprefixes to the classful network boundary when crossing classful network boundaries.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE auto-summary (RIP) command.

Examples

The following example show how to configure auto summary, where network numbers are not summarized automatically:

```
router rip
!
  version 2
```

```
  no auto-summary
!
```

default-information originate (RIP)

To generate a default route into Routing Information Protocol (RIP), use the **default-information originate** command in router configuration mode. To disable this feature, use the **no** form of this command.

default-information originate [**on-passive** | **route-map** *map-name*]
no default-information originate

Syntax Description

on-passive	(Optional) Sends default routes only on RIP-passive interfaces.
route-map *map-name*	(Optional) Specifies the routing process that is generating the default route if the route map is satisfied.

Command Default

No default routes are generated into RIP.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE default-information originate (RIP) command.

Examples

The following example shows how to configure a default originate route (0.0.0.0/0) over a certain interface when 172.17.0.0/16 is present. In this example a route map condition is applied:

```
router rip
 version 2
 network 172.17.0.0
 default-information originate route-map condition
!
route-map condition permit 10
 match ip address 10
 set interface s1/0
!
access-list 10 permit 172.17.0.0 0.0.255.255
!
```

default-metric (RIP)

To set default metric values for Routing Information Protocol (RIP), use the **default-metric** command in router configuration mode. To return to the default state, use the **no** form of this command.

default-metric *number-value*
no default-metric [*number-value*]

Syntax Description

number-value	Specifies default metric value.

Command Default

Default-metric is built-in, automatic metric translations, as appropriate, for each routing protocol.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE default-metric (RIP) command.

Examples

The following example shows how to configure a router in autonomous system 109 using both the RIP and Open Shortest Path First (OSPF) routing protocols. The example shows OSPF-derived routes advertisements using RIP and how to assign the OSPF-derived routes a RIP metric of 10:

```
router rip
!
  default-metric 10
  redistribute ospf 109
!
```

distance (IP)

To define an administrative distance for routes that are inserted into a routing table, use the **distance** command in router configuration mode. To return the administrative distance to its default distance definition, use the **no** form of this command.

distance *distance ip-address wildcard-mask* [*ip-standard-acl access-list-name*]
no distance *distance ip-address wildcard-mask* [*ip-standard-acl access-list-name*]

Syntax Description

distance	Administrative distance. Valid value is an integer from 10 to 255. (The values 0 to 9 are reserved for internal use. Routes with a distance value of 255 are not installed in the routing table.)
ip-address	IP address in four-part, dotted decimal notation. The IP address or the network address from where routes are learned.
wildcard-mask	Wildcard mask in four-part, dotted decimal notation. A bit set to 1 in the *wildcard-mask* argument instructs the software to ignore the corresponding bit in the address value.
ip -standard-acl	(Optional) Standard IP access list (ACL) number to be applied to incoming routing updates.
access-list-name	(Optional) Named access list to be applied to incoming routing updates.

Command Default

Default administrative RIP distance is 120.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE distance (ip) command.

Examples

In the following example, the **router rip** global configuration command sets up Routing Information Protocol (RIP) routing. The **network** router configuration command specify RIP routing on 192.168.7.0 and 172.16.0.0 networks. The first **distance** command sets the administrative distance to 90 for all routers on the Class C network 192.168.7.0. The second **distance** command sets the administrative distance to 120 for the router with the address 172.16.0.0.

```
config-transaction
!
  router rip
!
    network 192.168.7.0
    network 172.16.0.0
    distance 90 192.168.7.0 0.0.255.255
    distance 120 172.16.0.0 0.0.255.255
!
```

Table 41: Related Commands

Commands	Description
distance(IPv6)	Configures an administrative distance for IS-IS, RIP, or OSPF IPv6 routes inserted into the IPv6 routing table.
distance(ISO CLNS)	Configures the administrative distance for CLNS routes learned.
distancebgp	Allows the use of external, internal, and local administrative distances that could be a better route to a node.
distancebgp(IPv6)	Allows the use of external, internal, and local administrative distances that could be a better route than other external, internal, or local routes to a node.
distanceeigrp	Allows the use of two administrative distances--internal and external--that could be a better route to a node.
distanceospf	Defines OSPF route administrative distances based on route type.
showipprotocols	Displays the parameters and current state of the active routing protocol process.

distribute-list (RIP)

To filter the networks received in updates, to suppress networks from being advertised in updates, or to apply a prefix list to Routing Information Protocol (RIP) routing updates that are received or sent on an interface, use the **distribute-list** command in router configuration mode or address family configuration mode. To remove the prefix list, or to not filter updates, use the **no** form of this command.

distribute-list [*acl-number* | *expanded-acl-number* | *acl-name* | **gateway** *prefix-list-name* | **in** | **out** | **prefix** *listname*]
no distribute-list [*acl-number* | *expanded-acl-number* | *acl-name* | **gateway** *prefix-list-name* | **in** | **out** | **prefix** *listname*]

Syntax Description

acl-number	IP access list number. The acl-number argument defines which networks are to be received and which are to be suppressed in routing updates. Range is 1 to 199.
expanded-acl-number	IP-expanded access list number. Range is 1300 to 2699.
acl-name	IP access list name. The access-name argument defines which networks are to be received and which are to be suppressed in routing updates.
gateway	Filters incoming address updates based on a gateway.
prefix-list-name	IP prefix list name. This argument defines which routes from specified IP prefixes in the routing table are to be received and which are to be suppressed in routing updates.
in	Applies the prefix list to incoming routing updates on the specified interface.
out	Applies the prefix list to outgoing routing updates on the specified interface.
interface-type	(Optional) Specified interface type. For supported interface types, use the question mark (?) online help function.
interface-number	(Optional) Specified interface number.
prefix	Filters prefixes in routing address updates.
listname	Name of a prefix list. The list defines which IPv6 RIP networks are to be accepted in incoming routing updates and which networks are to be advertised in outgoing routing updates after matching the network prefix with the prefixes in the list.

Command Default

Networks that are received in updates are not filtered.

Command Modes

Router configuration (config-router)

Address family configuration (config-router-af)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE distribute-list prefix-list command.

Examples

The following example shows how to configure the distribute list prefix, which applies the prefix name prefix-list-1 to the Routing Information Protocol (RIP) routing updates that are received on GigabitEthernet interface 1/0/1:

```
router rip
!
    distribute-list prefix prefix-list-1 in GigabitEthernet 1/0/1
```

distribute-list prefix-list (IPv6 RIP)

To apply a prefix list to IPv6 Routing Information Protocol (RIP) routing updates that are received or sent on an interface, use the **distribute-list prefix-list** command in router configuration mode. To remove the prefix list, use the **no** form of this command.

distribute-list prefix-list *listname* { **in** | **out** }
no distribute-list prefix-list *listname*

Syntax Description

listname	Name of a prefix list. The list defines which IPv6 RIP networks are to be accepted in incoming routing updates and which networks are to be advertised in outgoing routing updates, based upon matching the network prefix to the prefixes in the list.
in	Applies the prefix list to IPv6 RIP incoming routing updates on the specified interface.
out	Applies the prefix list to IPv6 RIP outgoing routing updates on the specified interface.

Command Default

Prefix lists are not applied to IPv6 RIP routing updates.

Command Modes

Router configuration (config-rtr)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	This command was introduced.

Usage Guidelines

If no interface is specified, the prefix list is applied to all the interfaces.

For usage guidelines, see the Cisco IOS XE distribute-list prefix-list command.

Examples

The following example shows how to apply the prefix list named **cisco** to IPv6 RIP routing updates that are received on GigabitEthernet interface 0/0/0:

```
Device(config)# ipv6 router rip sdwan
Device(config-rtr)# distribute-list prefix-list cisco in GigabitEthernet0/0/0
```

input-queue

To define the number of received, but unprocessed Routing Information Protocol (RIP) update packets contained in the RIP input queue, use the **input-queue** command in router configuration mode. To remove the configured depth and restore the default depth, use the **no** form of this command.

input-queue *depth*
no input-queue

Syntax Description

depth	Numerical value associated with the maximum number of packets in a RIP input queue. The larger the numerical value, the larger the depth of the queue. The range is from 0 to 1024. The default is 150.

Command Default

Default depth value is 150.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE input-queue command.

Examples

The following example shows how to set the depth of a RIP input queue to 100:

```
router rip
!
  input-queue 100
!
```

ip rip advertise

To configure the interval at which Routing Information Protocol (RIP) updates are advertised from a specific RIP-enabled interface, use the **ip rip advertise** command in interface configuration mode. To remove the configured interval in which RIP updates are advertised from a specific RIP-enabled interface, use the **no** form of this command.

ip rip advertise *interval*
no ip rip advertise

Syntax Description

interval	Periodic advertisement interval, in seconds, at which RIP updates are sent from a specific RIP-enabled interface. The range is from 0 to 429466. The default is 30.

Command Default RIP updates are advertised every 30 seconds, which is the default global periodic interval for a Cisco device.

Command Modes Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines For usage guidelines, see the Cisco IOS XE ip rip advertise command.

Examples The following example shows how to configure the periodic advertisement interval on an interface:

```
config-transaction
  interface GigabitEthernet 1/0/1
!
    ip rip advertise 5
```

ip rip receive version

To specify the Routing Information Protocol (RIP) version that will be received on an interface, use the **ip rip receive version** command in interface configuration mode. To follow the global version rules, use the **no** form of this command.

ip rip receive version [**1**] [**2**]
no ip rip receive version

Syntax Description

1	(Optional) Accepts only RIP version 1 packets on the interface.
2	(Optional) Accepts only RIP version 2 packets on the interface.

Command Modes Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines For usage guidelines, see the Cisco IOS XE ip rip receive version command.

Examples The following example shows how to configure an interface to receive both RIP version 1 and version 2 packets:

```
config-transaction
  interface GigabitEthernet 1/0/1
!
   ip rip receive version 1 2
!
```

The following example shows how to configure an interface to receive only RIP version 1 packets:

```
config-transaction
  interface GigabitEthernet 1/0/1
!
   ip rip receive version 1
!
```

ip rip send version

To specify the Routing Information Protocol (RIP) version that will be sent on an interface, use the **ip rip send version** command in interface configuration mode. To follow the global version rules, use the **no** form of this command.

ip rip send version [**1**] [**2**]
no ip rip send version

Syntax Description

1	(Optional) Sends only RIP version 1 packets from the interface.
2	(Optional) Sends only RIP version 2 packets from the interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE ip rip send version command.

Examples

The following example shows how to configure an interface to send both RIP version 1 and version 2 packets from the interface:

```
config-transaction
  interface GigabitEthernet 1/0/1
!
   ip rip send version 1 2
!
```

The following example shows how to configure an interface to send only RIP version 2 packets from the interface:

```
config-transaction
  interface GigabitEthernet 1/0/1
!
   ip rip send version 2
!
```

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 (IP/length)* | **permit** *ipv6-prefix (IP/length)* | **description** *text*} [**ge** *ge-value*] [**le** *le-value*]
no ipv6 prefix-list *list-name*

Syntax Description

list-name	Name of the prefix list. • Cannot be the same name as an existing access list. • Cannot be **detail** or **summary** because these are keywords in the **show ipv6 prefix-list** command.
seq *seq-number*	(Optional) Sequence number of the prefix list entry being configured.
deny	Denies networks that don't match the condition.
permit	Permits networks that match the condition.
ipv6-prefix	The IPv6 network that is assigned to the specified prefix list. This argument must be in the form documented in RFC 2373, where the address is specified in hexadecimal format, using 16-bit values between colons.
(IP/length)	The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
description *text*	A description of the prefix list that can be up to 80 characters in length.
ge *ge-value*	(Optional) Specifies a prefix length greater than or equal to the *ipv6-prefix/prefix-length* arguments. It is the lowest value of a range of the *length* (*from* portion of the length range).
le *le-value*	(Optional) Specifies a prefix length less than or equal to the *ipv6-prefix /prefix-length* arguments. It is the highest value of a range of the *length* (*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 Catalyst SD-WAN Release 17.8.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE ipv6 prefix-list command.

Examples

The following example shows how to deny all routes with a prefix of ::/0:

```
Device(config)# ipv6 prefix-list abc deny ::/0
```

The following example shows how to permit 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 prefix—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 shows how to deny 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 shows how to permit mask lengths from 32 bits to 64 bits in all address spaces:

```
Device(config)# ipv6 prefix-list abc permit ::/0 ge 32 le 64
```

The following example shows how to deny mask lengths greater than 32 bits in all address spaces:

```
Device(config)# ipv6 prefix-list abc deny ::/0 ge 32
```

The following example shows how to deny all the routes with a prefix of 2002::/128:

```
Device(config)# ipv6 prefix-list abc deny 2002::/128
```

The following example shows how to permit all the routes with a prefix of ::/0:

```
Device(config)# ipv6 prefix-list abc permit ::/0
```

ipv6 rip default-information

To originate a default IPv6 route into Routing Information Protocol (RIP), use the **ipv6 rip default-information** command in interface configuration mode. To remove the default IPv6 RIP route, use the **no** form of this command.

ipv6 rip *ripng-instance* **default-information** { **only** | **originate** } [**metric** *metric-value*]
no ipv6 rip *ripng-instance* **default-information**

Syntax Description

ripng-instance	Name of the IPv6 RIP routing process. The only possible value is **sdwan**.
only	Advertises the IPv6 default route (::/0) only. Suppresses the advertisement of all other routes.

originate	Advertises the IPv6 default route (::/0). The advertisement of other routes is unaffected.
metric *metric-value*	(Optional) Associates a metric with the default route. The *metric-value* range is from 1 through 15.

Command Default

Metric value is 1.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE ipv6 rip default-information command.

Examples

The following example shows how a default IPv6 route distributed into RIPng on GigabitEthernet interface 0/0 and advertises only the default route in router updates that are sent on the interface:

```
Device(config)# interface GigabitEthernet 0/0
Device(config-if)# ipv6 rip sdwan default-information only
```

The following example shows how a default IPv6 route is distributed into RIPng on GigabitEthernet interface 0/0 and advertises the default route with all other routes in router updates that are sent on the interface:

```
Device(config)# interface GigabitEthernet 0/0
Device(config-if)# ipv6 rip sdwan default-information originate
```

ipv6 rip enable

To enable an IPv6 Routing Information Protocol (RIP) routing process on an interface, use the **ipv6 rip enable** command in interface configuration mode. To disable an IPv6 RIP routing process on an interface, use the **no** form of this command.

ipv6 rip *ripng-instance* **enable**
no ipv6 rip *ripng-instance*

Syntax Description

ripng-instance	Name of the IPv6 RIP routing process. The only possible value is **sdwan**.

Command Default

An IPv6 RIP routing process is not defined.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE ipv6 rip enable command.

Examples

The following example shows how to enable the IPv6 RIP routing process named sdwan on GigabitEthernet interface 0/1/0:

```
Device(config)# interface GigabitEthernet 0/1/0
Device(config-if)# ipv6 rip sdwan enable
```

ipv6 rip metric-offset

To set the IPv6 Routing Information Protocol (RIP) metric offset for an interface, use the **ipv6 rip metric-offset** command in interface configuration mode. To return the metric to its default value, use the **no** form of this command.

ipv6 rip *ripng-instance* **metric-offset** *offset value*
no ipv6 rip *ripng-instance* **metric-offset**

Syntax Description

ripng-instance	Name of the IPv6 RIP routing process. The only possible value is **sdwan**.
offset value	Specifies the offset value added to the metric of an IPv6 RIP route received in a report message. Range is from 1 to 16.

Command Default

The default metric offset value is 1.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE ipv6 rip metric-offset command.

Examples

The following example shows how to configure a metric offset increment of 10 for the RIP routing process named sdwan on GigabitEthernet interface 0/0:

```
Device(config)# interface GigabitEthernet 0/0
Device(config-if)# ipv6 rip sdwan metric-offset 10
```

ipv6 rip summary-address

To configure IPv6 Routing Information Protocol (RIP) to advertise summarized IPv6 addresses on an interface and to specify the IPv6 prefix that identifies the routes to be summarized, use the **ipv6 rip summary-address**

command in interface configuration mode. To stop advertising the summarized IPv6 addresses, use the **no** form of this command.

ipv6 rip *ripng-instance* **summary-address** *ipv6-prefix/prefix-length*
no ipv6 rip *ripng-instance* **summary-address**

Syntax Description

ripng-instance	Name of the IPv6 RIP routing process. The only possible value is **sdwan**.
ipv6-prefix	Specifies an IPv6 network number as the summary address. This argument must be in the format that is documented in RFC 2373, where the address is specified in hexadecimal using 16-bit values between colons.
/ *prefix-length*	The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.

Command Default

No default behavior or values.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE ipv6 rip summary-address command.

Examples

The following example shows how the IPv6 address 2001:0DB8:0:1:260:3EFF:FE11:6770 that is assigned to GigabitEthernet interface 0/0 with an IPv6 prefix length of 64 bits is summarized as IPv6 prefix 2001:0DB8::/35 for the IPv6 RIP routing process named sdwan:

```
Device(config)# interface GigabitEthernet 0/0
Device(config-if)# ipv6 address 2001:0DB8:0:1:260:3EFF:FE11:6770 /64
Device(config-if)# ipv6 rip sdwan summary-address 2001:90::1/32
```

ipv6 rip vrf-mode enable

To enable VRF-aware support for IPv6 Routing Information Protocol (RIP), use the **ipv6 rip vrf-mode enable** command in global configuration mode. To disable VRF-aware support for IPv6 RIP, use the **no** form of this command.

ipv6 rip vrf-mode enable
no ipv6 rip vrf-mode enable

Syntax Description

This command has no arguments or keywords.

Command Default

VRF-aware support is not enabled in IPv6 RIP.

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	This command was introduced.

Usage Guidelines When VRF-aware support is enabled in IPv6 RIP, you can configure only one RIP instance at a given time. More than one RIP instance is not allowed.

For usage guidelines, see the Cisco IOS XE ipv6 rip vrf-mode enable command.

Examples The following example shows how to enable VRF-aware support for IPv6 RIP routing:

```
Device(config)# ipv6 rip vrf-mode enable
Device(config)# ipv6 router rip sdwan
Device(config-rtr)# address-family ipv6 vrf 1
```

ipv6 router rip

To configure an IPv6 Routing Information Protocol (RIP) routing process, use the **ipv6 router rip** command in global configuration mode. To remove a routing process, use the **no** form of this command.

ipv6 router rip *ripng-instance*
no ipv6 router rip *ripng-instance*

Syntax Description

ripng-instance	Name of the RIPng instance that describes the routing process. The only possible value is **sdwan**.

Command Default No IPv6 RIP routing process is defined.

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	This command was introduced.

Usage Guidelines For usage guidelines, see the Cisco IOS XE ipv6 router rip command.

Examples The following example shows how to configure the IPv6 RIP routing process named sdwan and place the router in router configuration mode for the IPv6 RIP routing process:

```
Device(config)# ipv6 router rip sdwan
Device(config-rtr)# address-family ipv6 vrf 1
```

ipv6 unicast-routing

To enable the forwarding of IPv6 unicast datagrams, use the **ipv6 unicast-routing** command in global configuration mode. To disable the forwarding of IPv6 unicast datagrams, use the **no** form of this command.

ipv6 unicast-routing
no ipv6 unicast-routing

Syntax Description

This command has no arguments or keywords.

Command Default

IPv6 unicast routing is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE ipv6 unicast-routing command.

Examples

The following example shows how to enable the forwarding of IPv6 unicast datagrams:

```
Device(config)# ipv6 unicast-routing
```

maximum-paths

To control the maximum number of parallel routes that an IP routing protocol can support, use the **maximum-paths** command in router address family topology configuration mode or router configuration mode. To restore the default number of parallel routes, use the **no** form of this command.

maximum-paths *number-of-paths*
no maximum-paths *number-of-paths*

Syntax Description

number-of-paths	Maximum number of parallel routes that an IP routing protocol installs in a routing table. Valid values vary by Cisco IOS release and platform. For more information on valid values, use the question mark (**?**) online help function. The number-of-paths argument is an integer from 1 to 64. The default for RIP is 4 paths.

Command Default

The default number of parallel routes vary by Cisco IOS release and platform.

Command Modes

Router configuration (config-router)

Router address family topology configuration (config-router-af-topology)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE maximum-paths command.

Examples

The following example shows how to configure a maximum of 16 paths to be allowed to a destination in a RIP routing process:

```
config-transaction
!
  router rip
!
    maximum-paths 16
!
```

neighbor (RIP)

To define a neighboring router for exchanging routing information, use the **neighbor** command in router configuration mode. To remove a neighboring router entry, use the **no** form of this command.

neighbor *ip-address* [**bfd**]
no neighbor *ip-address* [**bfd**]

Syntax Description

ip-address	IP address of a peer router with which the routing information is exchanged.
bfd	(Optional) Sets the baseline Bidirectional Forwarding Detection (BFD) session parameters on an interface.

Command Default

No neighboring routers are defined.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE neighbor (RIP) command.

Examples

The following example shows how RIP updates are sent to all the interfaces on network 10.0.0.0 except GigabitEthernet interface 1/0/1. However, in this case, a **neighbor** router configuration command is included. The **neighbor** command permits the sending of routing updates to specific neighbors. One copy of the routing update is generated for each neighbor.

```
config-transaction
!
  router rip
!
```

```
    network 10.0.0.0
    passive-interface GigabitEthernet 1/0/1
    neighbor 10.108.20.4
!
```

The following example shows how to enable BFD for RIP neighbors:

```
config-transaction
!
  router rip
!
    neighbor 10.0.0.1 bfd
!
```

network (RIP)

To specify a list of networks for the Routing Information Protocol (RIP) routing process, use the **network** command in router configuration mode. To remove an entry, use the **no** form of this command.

network *ip-address*
no network *ip-address*

Syntax Description

ip-address	IP address of the network of directly connected networks.

Command Default

No networks are specified.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

Only classful IP network addresses are supported for network configuration. For usage guidelines, see the Cisco IOS XE network (RIP) command.

Examples

The following example shows how to configure a network that defines RIP as the routing protocol to be used on all the interfaces connected to networks 10.0.0.0 and 192.168.7.0:

```
config-transaction
!
  router rip
!
    network 10.0.0.0
    network 192.168.7.0
!
```

offset-list (RIP)

To add an offset to incoming and outgoing metric for routes learned through Routing Information Protocol (RIP), use the **offset-list** command in router configuration mode. To remove an offset list, use the **no** form of this command.

offset-list { *access-list-number* *expanded-access-list-number* *access-list-name* } { **in** *offset* | **out** *offset* } { *interface-type* *interface-name* }
no offset-list { *access-list-number* *expanded-access-list-number* *access-list-name* } { **in** *offset* | **out** *offset* } { *interface-type* *interface-name* }

Syntax Description

access-list-number	IP access list number. The access-list-number argument defines which networks are to be received and which are to be suppressed in routing updates. Range is 1 to 199.
expanded-acl-number	IP-expanded access list number. Range is 1300 to 2699.
access-list-name	Standard access list name to be applied.
in	Applies the access list to incoming metrics.
out	Applies the access list to outgoing metrics.
offset	Positive offset to be applied to metrics for networks matching the access list. If the offset is 0, no action is taken. Range is from 0 to 16.
interface-type	(Optional) Specified interface type. For supported interface types, use the question mark (?) online help function.
interface-number	(Optional) Specified interface number.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE offset-list (RIP) command.

Examples

The following example shows how a router applies an offset of 10 to the metric for routes matching access list 21:

```
config-transaction
!
  router rip
!
```

```
    offset-list 21 out 10
!
```

The following example shows how a router applies an offset of 10 to the routes learned from GigabitEthernet interface 1/0/1:

```
config-transaction
!
  router rip
!
   offset-list 21 in 10 GigabitEthernet 1/0/1
!
```

omp-route-tag

To enable automatic setting of the Routing Information Protocol version 2 (RIPv2)/Routing Information Protocol new generation (RIPng) route tag for the redistributed Overlay Management Protocol (OMP) routes, use the **omp-route-tag** command in router configuration mode or address family configuration mode. To disable this feature, use the **no** form of this command.

omp-route-tag
no omp-route-tag

Syntax Description

This command has no arguments or keywords.

Command Default

By default, **omp-route-tag** is enabled, and is not displayed in **show running-config**.

Command Modes

Router configuration (config-router)

Address family configuration (config-router-af)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

When a router is installed by another Cisco IOS XE Catalyst SD-WAN device, the admin distance is set to 252 so that OMP routes are preferred over redistributed OMP routes.

The **omp-route-tag** configuration is effective only on Cisco IOS XE Catalyst SD-WAN devices.

Examples

The following example shows how to enable automatic RIPv2 route tag for OMP routes in router configuration mode:

```
config-transaction
!
    router rip
!
      omp-route-tag
!
```

output-delay

To change the interpacket delay for the Routing Information Protocol (RIP) updates sent, use the **output-delay** command in router configuration mode. To remove the delay, use the **no** form of this command.

output-delay *delay*
no output-delay

Syntax Description

delay	Delay between packets in a multiple-packet RIP update, in milliseconds. The range is from 8 to 50. The default is 0.

Command Default

The default interpacket delay is 0 milliseconds.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE output-delay command.

Examples

The following example shows how to set the interpacket delay to 10 milliseconds:

```
config-transaction
!
  router rip
!
   output-delay 10
!
```

passive-interface

To disable the sending of routing updates on an interface, use the **passive-interface** command in router configuration mode. To re-enable the sending of routing updates, use the **no** form of this command.

passive-interface default [*interface-name*]
no passive-interface

Syntax Description

default	(Optional) Causes all the interfaces to become passive.
interface-name	(Optional) Interface name.

Command Default

Routing updates are sent on the interface.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE passive-interface command.

Examples

The following example shows how to configure an interface. RIP updates are sent to all the interfaces in the network 10.0.0.0 except GigabitEthernet interface 1/0/1:

```
config-transaction
!
  router rip
!
   network 10.0.0.0
   passive-interface GigabitEthernet 1/0/1
!
```

redistribute

To redistribute the specified routes into the Routing Information Protocol (RIP) routing process, use the **redistribute** command in the router configuration mode. To disable the configuration, use the **no** form of this command.

redistribute *protocol* [**metric** *Default-metric*] [**route-map** *map-tag*]
no redistribute *protocol*

Syntax Description

protocol	Protocol argument that can be one of these keywords—**bgp**, **connected**, **eigrp**, **isis**, **omp**, **ospf**, **ospfv3**, or **static**.
metric	Specifies the metric for redistributed routes.
Default-metric	Default metric value. Range is from 0 to 16.
route-map *map-tag*	Specifies the name of a route map that controls the redistribution.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Examples

The following example shows how to configure a router to redistribute OMP routes into a RIP process:

```
router rip
!
  redistribute omp metric 15 route-map x
```

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:

```
router ospf 109
 !
  redistribute eigrp 109 metric 100 subnets
  redistribute rip metric 200 subnets
```

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:

```
router rip
  !
  no redistribute connected metric 1000 subnets
```

The following example shows how to remove the **metric 5** option from the **redistribute static metric 5** command and leave the **redistribute static** command in the configuration:

```
router rip
  !
  no redistribute static metric 5
```

redistribute (IPv6)

To redistribute IPv6 routes from one routing domain into another routing domain, use the **redistribute** command in address family configuration or router configuration mode. To disable redistribution, use the **no** form of this command.

redistribute *source-protocol* [**metric** *metric-value*] [**route-map** *map-tag*]
no redistribute *source-protocol* [**metric** *metric-value*] [**route-map** *map-tag*]

Syntax Description

source-protocol	Source protocol from which routes are being redistributed. It can be one of the following keywords: **application**, **bgp**, **eigrp**, **isis**, **omp**, **static**, **lisp**, **nd**, **connected**, **ospf**, **ospfv3**.
metric *metric-value*	(Optional) Carries a metric from one process to the other if no metric value is specified when redistributing from one OSPF process to another OSPF process on the same router. When redistributing other processes to an OSPF process, the default metric is 20 when no metric value is specified.
route-map	(Optional) Specifies the route map that should be checked to filter routes from the source protocol as and when they are imported to the current routing protocol. If the **route-map** keyword is not specified, all the routes are redistributed. If this keyword is specified, but no route map tags are listed, no routes is imported.
map-tag	(Optional) Identifier of a configured route map.

Command Default

Route redistribution is disabled.

Command Modes

Address family configuration (config-ipv6-router-af)

Router configuration (config-rtr)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE redistribute ipv6 command.

Examples

The following example shows how to redistribute IPv6 BGP routes into the IPv6 RIP routing process named cisco:

```
Device(config)# ipv6 router rip cisco
Device(config-rtr)# redistribute bgp 42
```

The following example shows how to redistribute RIP for IPv6 routes into the OSPF for the IPv6 routing process:

```
Device(config)# ipv6 router ospf 1
Device(config-rtr)# redistribute rip 1 metric 32
```

The following example shows how to redistribute OMP routes for the IPv6 routing process:

```
Device(config-rtr)# address-family ipv6 vrf 1
Device(config-ipv6-router-af)# redistribute omp metric 10
```

router rip

To configure the Routing Information Protocol (RIP) routing process, use the **router rip** command in global configuration mode. To disable the RIP routing process, use the **no** form of this command.

router rip
no router rip

Syntax Description

This command has no arguments or keywords.

Command Default

No RIP routing process is defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE router rip command.

Examples

The following example shows how to configure a RIP router, which begins the RIP routing process:

```
config-transaction
```

```
!
  router rip
!
```

timers basic (RIP)

To adjust the Routing Information Protocol (RIP) network timers, use the **timers basic** command in router configuration mode. To reset the default timers, use the **no** form of this command.

timers basic *update invalid holddown flush*
no timers basic

Syntax Description

update	Rate, in seconds, at which updates are sent. This is the fundamental timing parameter of the routing protocol. The default is 30 seconds.
invalid	Interval of time, in seconds, after which a route is declared invalid; it should be at least three times the value of the *update* argument. A route becomes invalid when there is an absence of updates that refresh the route. The route then enters into a *holddown* state. The route is marked inaccessible and advertised as unreachable. However, the route is still used for forwarding packets. The default is 180 seconds.
holddown	Interval, in seconds, during which routing information regarding better paths is suppressed. It should be at least three times the value of the *update* argument. A route enters into a *holddown* state when an update packet, which indicates that the route is unreachable is received. The route is marked inaccessible and advertised as unreachable. However, the route is still used for forwarding packets. When holddown expires, routes advertised by other sources are accepted and the route is no longer inaccessible. The default is 180 seconds.
flush	Amount of time, in seconds, that must pass before the route is removed from the routing table; the interval specified should be greater than the value of the *invalid* argument. If it is less than this sum, the proper *holddown* interval cannot elapse, which results in a new route being accepted before the *holddown* interval expires. The default is 240 seconds.

Command Default

No RIP network timers are adjusted.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE timers basic (RIP) command.

Examples

The following example sets updates to be broadcast every 5 seconds. If a router does not respond within 15 seconds, the router is declared as unusable. Further information is suppressed for an additional 15 seconds, after which the route is flushed from the routing table:

```
router rip
!
```

```
  timers basic 5  15  15  30
!
```

Note By setting a short update period, you run the risk of congesting slow-speed serial lines. A short update period can be a concern on faster-speed Ethernets and T1-rate serial lines. Also, if you have many routes in your updates, you can cause the routers to spend an excessive amount of time processing updates.

The following example shows how to adjust address family timers:

```
router rip
 version 2
 timers basic 5 10 15 20
 redistribute connected
 network 5.0.0.0
 default-metric 10
  no auto-summary
  !
  address-family ipv4 vrf 1
   timers basic 10 20 20 20
   redistribute connected
   network 10.0.0.0
   default-metric 5
   no auto-summary
   version 2
   exit-address-family
  !
  address-family ipv4 vrf 1
   timers basic 20 40 60 80
   redistribute connected
   network 20.0.0.0
   default-metric 2
   no auto-summary
   version 2
   exit-address-family
 !
```

traffic-share min

To configure traffic to use minimum-cost routes when there are multiple routes that have different-cost routes to the same destination network, use the **traffic-share min** command in router address family topology configuration mode or router configuration mode. To disable this function, use the **no** form of this command.

traffic-share min across-interfaces
no traffic-share min across-interfaces

Syntax Description

across-interfaces	Configures multiinterface load splitting on several interfaces with equal-cost paths.

Command Default

Traffic is configured to use minimum-cost paths.

Command Modes

Router configuration (config-router)

Router address family topology configuration (config-router-af-topology)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE traffic-share min command.

Examples

The following example shows multiinterface load splitting configuration on different interfaces with equal-cost paths:

```
router rip
!
    traffic-share min across-interfaces
!
```

validate-update-source

To have the Cisco IOS software validate the source IP address of incoming routing updates for the Routing Information Protocol (RIP) routing protocols, use the **validate-update-source** command in router configuration mode. To disable this function, use the **no** form of this command.

validate-update-source
no validate-update-source

Syntax Description

This command has no arguments or keywords.

Command Default

The behavior of this command is enabled by default.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE validate-update-source command.

Examples

The following example configures a router to not perform validation checks on the source IP address of incoming RIP updates:

```
router rip
!
  network 10.0.0.0
  no validate-update-source
!
```

version (RIP)

To specify a Routing Information Protocol (RIP) version used globally by the router, use the **version** command in router configuration mode. To restore the default value, use the **no** form of this command.

version { **1** | **2** }
no version

Syntax Description

1	Specifies RIP version 1.
2	Specifies RIP version 2.

Command Default

The software receives RIP version 1 and version 2 packets, but sends only version 1 packets.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

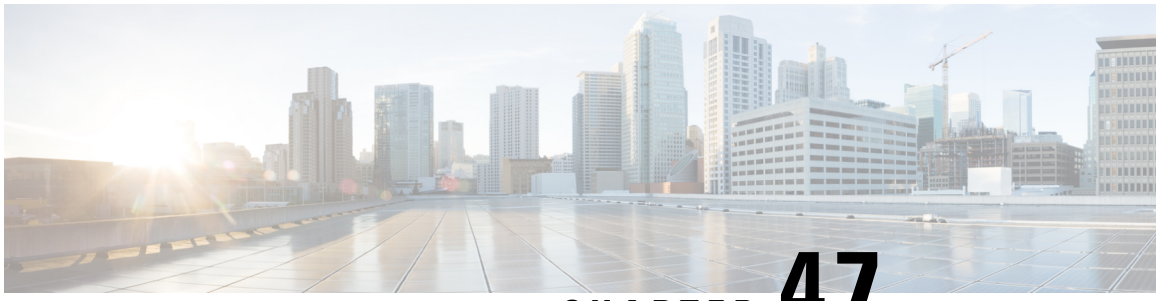
Usage Guidelines

For usage guidelines, see the Cisco IOS XE version command.

Examples

The following example shows how to configure version 2, which enables the software to send and receive RIP version 2 packets:

```
router rip
!
  version 2
!
```



CHAPTER 47

Routemap Commands

•
• ipv6 policy route-map, on page 693
• match ip address, on page 694
• match length, on page 695
• set community, on page 696
• route-map permit set default interface, on page 697
• route-map permit set interface, on page 698
• route-map permit set ipv6 precedence, on page 699
• set origin, on page 700
• route-map permit set vrf, on page 701
• route-map, on page 702

ipv6 policy route-map

To set an interface to use policy-based routing (PBR) with IPv6, use the **ipv6 policy route-map** command in interface configuration mode. To clear the PBR, use the **no** form of this command.

ipv6 policy route-map *string*
no ipv6 policy route-map *string*

Syntax Description

string	Identifies a route map to be used for IPv6 PBR on an interface.

Command Default

None

Command Modes

interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

To enable PBR for IPv6, create a route map that specifies the packet match criteria and the desired policy-route action. Then, associate the route map on the required interface. All packets arriving on the specified interface that match the match clauses will be subject to PBR.

Depending on your release, IPv6 PBR allows users to override normal destination IPv6 address-based routing and forwarding results. VPN routing and forwarding (VRF) allows multiple routing instances in Cisco software. The PBR feature is VRF-aware, which means that it works under multiple routing instances, beyond the default or global routing table.

Example

The following example configures PBR on GigabitEthernet 0/0/2, using the map tag "rip-to-ospf"

```
Device(config)# interface GigabitEthernet 0/0/2
Device(config-if)# ipv6 policy route-map rip-to-ospf
```

match ip address

To distribute any routes that have a destination IP network number address that is permitted by a standard access list, an expanded access list, or a prefix list, use the **match ip address** command. To remove the **match ip address** entry, use the **no** form of this command.

match ip address { **prefix-list** | [*prefix-list-name*] }

no match ip address { **prefix-list** | [*prefix-list-name*] }

Syntax Description

prefix-list*prefix-list-name*	Distributes routes based on a prefix list. The prefix list name can be any alphanumeric string up to 63 characters. The ellipsis indicates that multiple values can be entered, up to 32 prefix lists.

Note In Cisco Catalyst SD-WAN Manager Release 20.15.1, when pushing a CLI template to a device running a version earlier than Cisco Catalyst SD-WAN Manager Release 20.15.1, the CLI template must include the following configuration lines under route-map:

```
match ip address prefix-list xyz
match ip address prefix-list-deprecated xyz
match ip address 33
match ip address access-list 33
```

Command Default

No prefix lists are specified.

Command Modes

Route-map configuration mode (config-route-map)

Command History

Note In Cisco Catalyst SD-WAN Manager Release 20.15.1, when pushing a CLI template to a device running a version earlier than Cisco Catalyst SD-WAN Manager Release 20.15.1, the CLI template must include the following configuration lines under route-map:

```
description SET COMMUNITY FOR EDGE ROUTES
description-deprecated SET COMMUNITY FOR EDGE ROUTES
```

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Examples

This example shows how to match routes that have addresses specified by an access list test:

```
Device(config)# route-map rmap1 deny 10
Device(config-route-map)# match ip address prefix-list prfx1
```

match length

To base policy routing on the Level 3 length of a packet, use the **match length** command in route-map configuration mode. To remove the entry, use the **no** form of this command.

match length *minimum-length maximum-length*
no match length *minimum-length maximum-length*

Syntax Description

minimum-length	Minimum Level 3 length of the packet allowed for a match. The range is from 0 to 2147483647.
maximum-length	Maximum Level 3 length of the packet allowed for a match. The range is from 0 to 2147483647.

Command Default

No policy routing occurs on the length of a packet.

Command Modes

Route-map configuration (config-route-map)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE match length command.

Examples

In the following example, packets 3 to 200 bytes long, inclusive, will be routed to FDDI interface 0:

```
Router(config)# interface Ethernet0/0
(config-router)# route-map interactive
Router(config-route-map) match length 3 200
Router(config-route-map) set interface fddi 0
```

set community

To set the BGP communities attribute, use the **set community** route map configuration command in route-map configuration mode. To delete the entry, use the **no** form of the command.

set community community-deprecated { *community-number* [**additive**] [*well-known-community*] | **none** }

no set community

Syntax Description

community-deprecated	This keyword is provided for backward compatibility. Use this keyword if you are using Cisco Catalyst SD-WAN Manager Release 20.15.1 and later with Cisco IOS XE Catalyst SD-WAN devices running 17.14.x or earlier.
community-number	Community number. Range: 1 to 4,294,967,200
additive	(Optional) Adds the community to the already existing communities.
well-known-community	(Optional) Well know communities can be specified by using the following keywords: • *internet* • *local-as* • *no-advertise* • *no-export*
none	(Optional) Removes the community attribute from the prefixes that match the route map.

Command Default

No BGP communities attributes exist.

Command Modes

route map configuration (config-route-map)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.15.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

You must have a match clause to set tags, even if you want to permit all routes without filtering any out.

To define the conditions for redistributing routes from one routing protocol into another, use the **route-map** global configuration command, with the **match** and **set** route-map commands.

Each **route-map** command has a list of **match** and **set** commands associated with it:

- The **match** command specifies the match criteria–the conditions under which redistribution is allowed for the current **route-map** command.
- The **set** command specifies the set actions–the redistribution action to perform if the criteria enforced by the **match** commands are met.

The **no route-map** command deletes the route map.

Examples

In the following example, a device finds routes that match autonomous system path access list 1 and sets community to *109*. Similarly, the device finds routes that match autonomous system path access list 2 and sets the community to *no-export* community (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
```

If you are using Cisco Catalyst SD-WAN Manager Release 20.15.1 and later with Cisco IOS XE Catalyst SD-WAN devices running 17.14.x or earlier, use the **community-deprecated** keyword for backward compatibility:

```
route-map set_community permit 10
set community community-deprecated 13:1001
```

route-map permit set default interface

To set the output interface for destinations that match the criteria in the route-map, if there is no explicit route to the destination, use the **set default interface** command in route-map configuration mode. To delete an entry, use the **no** form of this command.

route-map *route-map* **permit** *value* [**set default interface** *string*]
no route-map *route-map* **permit** *value* [**set default interface** *string*]

Syntax Description

route-map	A name specified for the specific route-map.
value	Sets the value of the permit or deny action of the route-map.
string	Interface type, and interface number, to which packets are forwarded. IE. GigabitEthernet, Tunnel.

Command Default

This command is disabled by default.

Command Modes route map configuration (config-route-map)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the type and number arguments.

If the first interface specified with the set interface command is down, the optionally specified interfaces are tried in turn. If no other interface is specified, the default interface is then used.

Example

The following example configures the route-map "rip-to-ospf" to forward packets that pass the match criteria to the default interface of Tunnel1 if no other interface is specified.

```
Device(config)# route-map rip-to-ospf permit 79
Device(config-route-map)# set default interface Tunnel1
```

The following example configures the route-map "rip-to-ospf" to forward packets that pass the match criteria to the default interface of GigabitEthernet 3 if no other interface is specified.

```
Device(config)# route-map rip-to-ospf permit 56
Device(config-route-map)# set default interface GigabitEthernet 0/0/3
```

route-map permit set interface

To set the output interface for destinations that match the criteria in the route-map, use the **set default interface** command in route-map configuration mode. To delete an entry, use the **no** form of this command.

route-map *route-map* **permit** *value* [**set interface** *string*]
no route-map *route-map* **permit** *value* [**set interface** *string*]

Syntax Description

route-map	A name specified for the specific route-map.
value	Sets the value of the permit or deny action of the route map.
string	Interface type, and interface number, to which packets are forwarded. For example, GigabitEthernet or Tunnel.

Command Default Packets that pass a match clause are not forwarded to an interface.

Command Modes route map configuration (config-route-map)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the type and number arguments.

If the first interface specified with the set interface command is down, then the optionally specified interfaces are used instead.

Example

The following example configures the route-map "rip-to-ospf" to forward packets that pass the match criteria to interface Dialer1.

```
Device(config)# route-map rip-to-ospf permit 50
Device(config-route-map)# set interface Dialer1
```

The following example configures the route-map "rip-to-ospf" to forward packets that pass the match criteria to interface GigabitEthernet 2.

```
Device(config)# route-map rip-to-ospf permit 55
Device(config-route-map)# set interface GigabitEthernet 0/0/2
```

The following example configures the route-map "rip-to-ospf" to forward packets that pass the match criteria to interface tunnel1.

```
Device(config)# route-map rip-to-ospf permit 60
Device(config-route-map)# set interface Tunnel
```

route-map permit set ipv6 precedence

To set a IPv6 precedence value, use the **set ipv6 precedence** command in route map configuration mode. To clear the IPv6 precedence, use the **no** form of this command.

route-map *route-map* **permit** *value* **set ipv6 precedence** *unsigned-byte*
no route-map *route-map* **permit** *value* **set ipv6 precedence** *unsigned-byte*

Syntax Description

route-map	A name specified for the specific route-map.
value	Sets the value for the permit or deny action of the route map.
unsigned-byte	Sets precedence value in the ipv6 header.The range is from 0 to 7.

Command Default

None

Command Modes

route map configuration (config-route-map)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

When creating a route map that specifies the packet match criteria and desired policy-route action, you can specify the IPv6 precedence header value for the route-map policy.

Example

The following example configures IPv6 precedence value of 3 for the “rip-to-ospf” route map.

```
Device(config)# route-map rip-to-ospf permit 45
Device(config-route-map)# set ipv6 precedence 3
```

Table 42: Related Commands

Commands	Description
set ipv6 address	IPv6 address.
set ipv6 bvrf	Sets VRF instance selection within a route map for a policy-based routing VRF selection.
set ipv6 default	Sets default parameters for the policy.
set ipv6 global	Sets global parameters for the policy.
set ipv6 next-hop	Sets next hop to route the packet (the next hop must be adjacent).

set origin

To set the BGP origin code, use the **set origin** command in route-map configuration mode. To delete an entry, use the **no** form of this command.

set origin origin-v1 { **igp** | **egp** *autonomous-system-number* | **incomplete** }

no set origin { **igp** | **egp** *autonomous-system-number* | **incomplete** }

Syntax Description

origin-v1	This keyword is provided for backward compatibility. Use this keyword if you are using Cisco Catalyst SD-WAN Manager Release 20.15.1 and later with Cisco IOS XE Catalyst SD-WAN devices running 17.14.x or earlier.
igp	Remote Interior Gateway Protocol (IGP) system.
egp	Local Exterior Gateway Protocol (EGP) system.
autonomous-system-number	Remote autonomous system number. Range:1 to 65535
incomplete	Origin of the route is unknown.

Command Default

The origin of the route is based on the path information of the route in the main IP routing table.

Command Modes

route map configuration (config-route-map)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.15.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

You must have a match clause to set the origin of a route, even if you want to permit all routes without filtering any out.

Use this command to set a specific origin when a route is redistributed into BGP. When routes are redistributed, the origin is usually recorded as incomplete, identified with a ? in the BGP table.

To define the conditions for redistributing routes from one routing protocol into another, use the **route-map** global configuration command, with the **match** and **set** route-map commands.

Each **route-map** command has a list of **match** and **set** commands associated with it:

- The **match** command specifies the match criteria–the conditions under which redistribution is allowed for the current **route-map** command.
- The **set** command specifies the set actions–the redistribution action to perform if the criteria enforced by the **match** commands are met.

The **no route-map** command deletes the route map.

Examples

This example sets the origin of routes that pass the route map to IGP:

```
route-map set_origin
 match as-path 10
 set origin igp
```

If you are using Cisco Catalyst SD-WAN Manager Release 20.15.1 and later with Cisco IOS XE Catalyst SD-WAN devices running 17.14.x or earlier, use the **origin-v1** keyword for backward compatibility:

```
route-map set_origin
match as-path 10
set origin-v1 igp
```

route-map permit set vrf

To use a specific VRF table for Policy-based routing (PBR), use the **route-map permit set vrf** command in route map configuration mode. To remove the VRF from the route-map, use the **no** form of this command.

route-map *route-map* **permit** *value* **set vrf** *string*

Syntax Description

route-map	A name specified for the specific route-map.
value	Sets the value for the permit or deny action of the route map.
string	A name specified for a specific VRF.

Command Default

None

Command Modes

route map configuration (config-route-map)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Use **route-map permit set vrf** command to route packets using a particular VRF table through any of the interfaces belonging to that VRF. If there is no route in the VRF table, the packets are dropped.

Example

The following example configures a VRF-aware PBR, using the map tag “rip-to-ospf”.

```
Device(config)# route-map rip-to-ospf permit 70
Device(config-route-map)# set vrf mgmt
```

route-map

To define conditions for redistributing routes from one routing protocol to another routing protocol, or to enable policy routing, use the **route-map** command in global configuration mode. To delete an entry, use the **no** form of this command.

route-map *map-name* [**permit** | **deny**] *sequence-number*
no route-map *map-name* [**permit** | **deny**] *sequence-number*

Syntax Description

map-name	Name for the route map.
permit	(Optional) Permits only routes matching the route map to be forwarded or redistributed.
deny	(Optional) Blocks routes matching the route map from being forwarded or redistributed.
sequence-number	(Optional) Number that indicates the position a new route map will have in the list of route maps already configured with the same name.

Command Default

Policy routing is not enabled and conditions for redistributing routes from one routing protocol to another routing protocol are not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE route-map command.

Note In Cisco Catalyst SD-WAN Manager Release 20.15.1, when pushing a CLI template to a device running a version earlier than Cisco Catalyst SD-WAN Manager Release 20.15.1, the CLI template must include the following configuration lines under route-map:

```
match ip address prefix-list xyz
match ip address prefix-list-deprecated xyz
match ip address 33
match ip address access-list 33
```

Examples

The following is an example for this command:

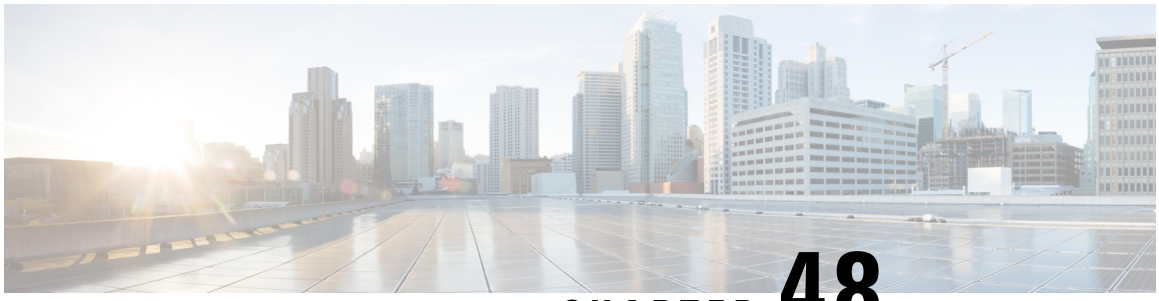
```
Device(config)# route-map ospf deny 10
Device(config)# route-map rip permit 10
```

The following example redistributes Routing Information Protocol (RIP) routes with a hop count equal to 1 into Open Shortest Path First (OSPF). These routes will be redistributed into OSPF as external link-state advertisements (LSAs) with a metric of 5, metric type of Type 1, and a tag equal to 1.

```
Router(config)# router ospf 109
Router(config-router)# redistribute rip route-map rip-to-ospf
Router(config-router)# exit
Router(config)# route-map rip-to-ospf permit
Router(config-route-map)# match metric 1
Router(config-route-map)# set metric 5
Router(config-route-map)# set metric-type type1
Router(config-route-map)# set tag 1
```

The following example for IPv6 redistributes RIP routes with a hop count equal to 1 into OSPF. These routes will be redistributed into OSPF as external LSAs with a tag equal to 42 and a metric type equal to type1.

```
Router(config)# ipv6 router ospf 1
Router(config-router)# redistribute rip one route-map rip-to-ospfv3
Router(config-router)# exit
Router(config)# route-map rip-to-ospfv3
Router(config-route-map)# match tag 42
Router(config-route-map)# set metric-type type1
```



CHAPTER 48

Routing

- affinity-per-vrf, on page 705
- affinity-group preference-auto, on page 706
- redistribute omp translate-rib-metric, on page 707

affinity-per-vrf

Use the **affinity-per-vrf** command in system configuration mode to configure a device to have an affinity value for traffic in a specific VRF or range of VRFs. Use the **no** form of the command to remove this configuration.

affinity-per-vrf *affinity-value* **vrf-range** *vrf-range*

no affinity-per-vrf

Syntax Description

affinity-per-vrf *affinity-value*	Affinity group to use for the VRF range.
vrf-range *vrf-range*	A single VRF value or range of values, separated by a hyphen. This parameter does not support a comma-separated list of individual VRF values. Examples: 1 3-6

Command Default

Disabled

Command Modes

System (config-system)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	This command was introduced.

Usage Guidelines

Specifying affinity group numbers for specific VRFs provides granular control of how routers choose the next hop for traffic in different VRFs.

Example

The following example configures affinity group 1 for VRF1:

```
Device(config)#system
Device (config-system)# affinity-per-vrf 1 vrf-range 1
```

Example

The following example configures affinity group 4 for the VRF range 3 to 6:

```
Device(config)#system
Device (config-system)# affinity-per-vrf 4 vrf-range 3-6
```

Related Commands

Command	Description
affinity-group	Configures an affinity group for a router.
affinity-group preference	Configures the affinity group preference order, from highest priority to lowest priority.

affinity-group preference-auto

Use the **affinity-group preference-auto** command in system configuration mode to configure a device to choose a next hop to a device with the lowest possible affinity group number. Use the **no** form of the command to remove this configuration.

affinity-group preference-auto

no affinity-group preference-auto

Command Default

Disabled

Command Modes

System (config-system)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	This command was introduced.

Usage Guidelines

As an alternative to the **affinity-group preference** command, which specifies affinity groups in order of preference, the **affinity-group preference-auto** command configures a device to choose a next hop to a device with the lowest possible affinity group number. Affinity group 1 has a higher priority than affinity group 2, and so on.

If you configure a router with both **affinity-group preference-auto** and **affinity-group preference** *list*, the **affinity-group preference-auto** command has priority for selecting a next hop. However, the **affinity-group preference** *list* command is still useful for path filtering using the **filter route outbound affinity-group**

preference command. For information about filtering out paths for routers that are not on the device's affinity list, see Information About Router Affinity Groups and see the filter route outbound affinity-group preference command reference.

Example

```
Device(config)#system
Device (config-system)# affinity-group preference-auto
```

Related Commands

Command	Description
affinity-group	Configures an affinity group for a router.
affinity-group preference	Configures the affinity group preference order, from highest priority to lowest priority.
filter route outbound affinity-group preference	Configures a Cisco SD-WAN Controller to restrict routers in the regions that it is managing to connect only to routers that are on their affinity list.

redistribute omp translate-rib-metric

Use the **redistribute omp translate-rib-metric** command in router configuration mode or address family configuration mode to configure a device to translate Overlay Management Protocol (OMP) route metrics for use with devices outside of the overlay network that use either the border gateway protocol (BGP) or open shortest path first (OSPF) protocol for the control plane. Use the **no** form of the command to remove this configuration.

redistribute omp translate-rib-metric
metric *metric*

no redistribute omp translate-rib-metric

Syntax Description

metric *metric*	Manually assign a metric value to a route. Routers prioritize routes with a lower value. Do not use this option together with **redistribute omp translate-rib-metric**. Range: 1 to 2^24–1

Command Default

Disabled

Command Modes

Router configuration mode (config-router)
Address family configuration mode (config-router-af)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	This command was introduced.

Usage Guidelines

Devices within the Cisco Catalyst SD-WAN overlay network use OMP for control plane information. Outside of the overlay, devices use other control plane protocols such as BGP or OSPF. A device at the interface between devices within the overlay network and devices outside of the overlay can translate OMP route metrics when redistributing routes to BGP or OSPF, to be usable by devices outside the overlay network.

An example is a router managed by Cisco Catalyst SD-WAN, serving as a hub for a data center. Data center routers may be outside of the overlay network. For traffic between the hub and the data center routers, it is helpful to translate route metrics from OMP to BGP. This enables the data center routers to make best path calculations that use the route metrics from the overlay network. In turn, this enables functionality such as preserving route symmetry, meaning that for traffic flows between the hub and data center routers, traffic in both directions can use the same route. For information, see Symmetric Routing in the Cisco Catalyst SD-WAN Routing Configuration Guide, Cisco IOS XE Release 17.x.



Note You cannot use both the **redistribute omp translate-rib-metric** command and the **redistribute omp metric metric-value** command together on the same device.

Example: BGP

This example applies to a scenario in which the underlay network uses BGP:

```
Device(config)#router bgp 1
Device(config-router)#address-family ipv4 vrf 2
Device(config-router-af)#redistribute omp translate-rib-metric
```

Example: OSPF

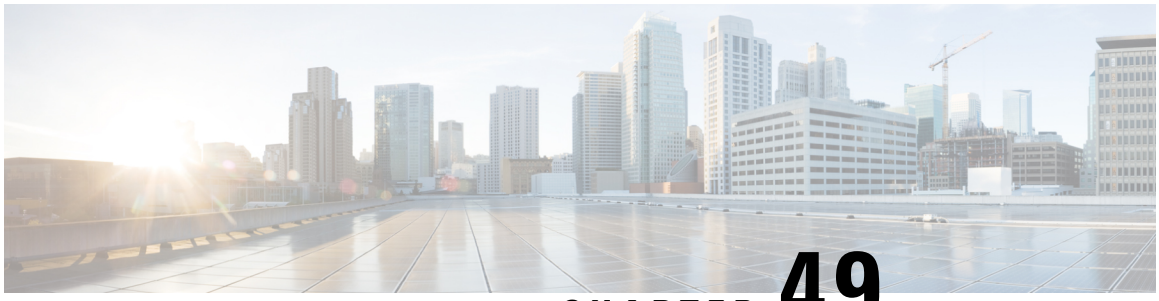
This example applies to a scenario in which the underlay network uses OSPF:

```
Device(config)#router ospf 1
Device(config-router)#redistribute omp translate-rib-metric
```

Example: OSPFv3

his example applies to a scenario in which the underlay network uses OSPFv3:

```
Device(config)#router ospf3 1
Device(config-router)#address-family ipv4 vrf 2
Device(config-router-af)#redistribute omp translate-rib-metric
```



CHAPTER 49

SD-WAN Tunnel Interface Commands

- access-list, on page 709
- allow-service, on page 710
- auto-bandwidth-detect, on page 712
- bandwidth-downstream, on page 712
- bandwidth-upstream, on page 714
- carrier, on page 714
- color, on page 715
- encapsulation, on page 716
- gre-in-udp, on page 717
- exclude-controller-group-list, on page 718
- hello-interval, on page 719
- hello-tolerance, on page 720
- iperf-server, on page 721
- last-resort-circuit, on page 722
- low-bandwidth-link, on page 723
- max-control-connections, on page 724
- nat-refresh-interval, on page 725
- port-hop, on page 726
- tloc-extension, on page 727
- tunnel-interface, on page 727
- vbond-as-stun-server, on page 728
- vmanage-connection-preference, on page 729

access-list

To apply an access list to an interface, use the **access-list** command in the SD-WAN physical interface configuration mode. To remove the access list, use the **no** form of the command.

access-list *acl-name* { **in** | **out** }

no access-list *acl-name* { **in** | **out** }

Syntax Description

acl-name	Name of the access list to apply to the interface.

in | **out**	Direction in which to apply the access list. Applying it in the inbound direction (**in**) affects packets being received on the interface. Applying it in the outbound direction (**out**) affects packets being transmitted on the interface.

Command Default

An access list is not applied to an interface.

Command Modes

SD-WAN physical interface configuration mode (config-interface-*interface-name*)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

Example

```
Device(config)# sdwan

Device(config-sdwan)# interface ge0/2.101

Device(config-interface-ge0/2.101)# access-list acl1 in
```

allow-service

To configure the services that are allowed on a tunnel interface, use the **allow-service** command in tunnel interface configuration mode. To disallow a service on a tunnel interface, use the **no** form of the command.

allow-service *service-name*

no allow-service *service-name*

Syntax Description

service-name	Type of service to allow or disallow on the WAN tunnel connection. *service-name* can be **all** or one of more of **bfd**, **bgp**, **dhcp**, **dns**, **https**, **icmp**, **netconf**, **ntp**, **ospf**, **sshd**, and **stun**. By default, DHCP (for DHCPv4 and DHCPv6), DNS, HTTPS, and ICMP are enabled on a tunnel interface. You cannot disallow the following services: DHCP, DNS, NTP, and STUN. If you allow the NTP service on the tunnel interface, you must configure the address of an NTP server with the **system ntp** command. The **allow-service stun** command pertains to allowing or disallowing a Cisco IOS XE SD-WAN device to generate requests to a generic STUN server so that the device can determine whether it is behind a NAT and, if so, what kind of NAT it is and what the device's public IP address and public port number are. On a Cisco IOS XE SD-WAN device that is behind a NAT, you can also have tunnel interface to discover its public IP address and port number from the Cisco vBond orchestrator, by configuring the **vbond-as-stun-server** command on the tunnel interface. To configure more than one service, include multiple **allow-service** commands. Configuring **allow-service all** overrides any commands that allow or disallow individual services. **Note** Starting from Cisco IOS XE Catalyst SD-WAN Release 17.16.1a, configuring **allow-service all** on Cisco Catalyst SD-WAN Controllers is only applicable for the following services **bgp**, **dhcp**, **dns**, **https**, **icmp**, **netconf**, **ntp**, **ospf**, **sshd**, and **stun**.

Command Default

By default, DHCP (for DHCPv4 and DHCPv6), DNS, HTTPS, and ICMP are enabled on a tunnel interface.

Command Modes

tunnel interface configuration mode (config-tunnel-interface)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

Example

```
Device(config)# sdwan

Device(config-sdwan)# interface GigabitEthernet1

Device(config-interface-GigabitEthernet1)# tunnel-interface
Device(config-tunnel-interface)# no allow-service all
Device(config-tunnel-interface)# no allow-service bgp
Device(config-tunnel-interface)# allow-service dhcp
Device(config-tunnel-interface)# allow-service dns
Device(config-tunnel-interface)# allow-service icmp
Device(config-tunnel-interface)# no allow-service sshd
Device(config-tunnel-interface)# no allow-service netconf
Device(config-tunnel-interface)# no allow-service ospf
Device(config-tunnel-interface)# allow-service https
Device(config-tunnel-interface)# no allow-service netconf
Device(config-tunnel-interface)# no allow-service snmp
```

auto-bandwidth-detect

Configure a device to automatically detect the bandwidth for WAN interfaces in VPN0 during day 0 onboarding. The device detects the bandwidth by contacting an iPerf3 server to perform a speed test. To remove the configuration, use the **no** form of this command.

auto-bandwidth-detect
no auto-bandwidth-detect

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes SD-WAN physical interface configuration mode (config-interface-*interface-name*)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	This command was introduced.

Usage Guidelines Use the auto-bandwidth-detect to configure a device to automatically detect the bandwidth for the VPN interface when the device boots up and connects to Cisco SD-WAN Manager after completing the PnP process. By default, the device uses a public iPerf3 server to perform a speed test for bandwidth detection. You can specify a private iPerf3 server to use instead by using the iperf-server command.

The private iPerf3 server should run on port 5201, which is the default iPerf3 port.

Example

The following example shows how to enable automatic bandwidth detection:

```
Device(config)# sdwan
Device(config-sdwan)# interface GigabitEthernet
Device(config-interface-GigabitEthernet) auto-bandwidth-detect
```

Table 43: Related Commands

Command	Description
iperf-server	Specifies a local iPerf3 server that a device contacts to perform a speed test for automatic bandwidth detection.

bandwidth-downstream

To generate notifications when the bandwidth of traffic received on a physical interface in the WAN transport VPN (VPN 0) exceeds a specific limit, use the **bandwidth-downstream** command in the SD-WAN physical interface configuration mode.

Notifications are generated when traffic exceeds 85 percent of the bandwidth you configure with this command. To stop notification generation, use the **no** form of the command.

bandwidth-downstream *kbps*

no bandwidth-downstream

Syntax Description

kbps	Maximum received on a physical interface to allow before generating a notification. When the transmission rates exceeds 85 percent of this rate, an SNMP trap is generated. Range: 1 through 2147483647 kbps

Command Default

By default, bandwidth notifications are not generated.

Command Modes

SD-WAN physical interface configuration mode (config-interface-*interface-name*)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.
Cisco IOS XE Catalyst SD-WAN Release 17.16.1a	From Cisco IOS XE Catalyst SD-WAN Release 17.2.1v through 17.15.x, the **bandwidth-downstream** command works only if you have also configured per-tunnel QoS for the device. From Cisco IOS XE Catalyst SD-WAN Release 17.16.1a the **bandwidth-downstream** command works even without configuring per-tunnel QoS.

Usage Guidelines

Notifications generated include Netconf notifications, which are sent to Cisco SD-WAN Manager, SNMP traps, and syslog messages. Notifications are sent when the received bandwidth exceeds 85 percent of the bandwidth configured for that type of traffic.

A second use of **bandwidth-downstream** command is for enabling per-tunnel QoS, together with the **tunnel-qos spoke** command. For more information about enabling QoS, see Per-Tunnel QoS.

Example

```
Device(config)# sdwan

Device(config-sdwan)# interface GigabitEthernet1

Device(config-interface-GigabitEthernet1)# bandwidth-downstream 300000000
```

Related Commands

Command	Description
bandwidth-upstream	Generates notifications when the bandwidth of traffic transmitted on a physical interface exceeds 85% of the configured bandwidth reference value.

bandwidth-upstream

To generate notifications when the bandwidth of traffic transmitted on a physical interface exceeds a specific limit, use the **bandwidth-upstream** command.

Notifications are generated when traffic exceeds 85 percent of the bandwidth you configure with this command. To stop notification generation, use the **no** form of the command.

bandwidth-upstream *kbps*

no bandwidth-upstream

Syntax Description

kbps	Maximum kbps transmitted on a physical interface to allow before generating a notification. When the transmission rates exceeds 85 percent of this rate, an SNMP trap is generated. Range: 1 through 2147483647 kbps

Command Default

By default, bandwidth notifications are not generated.

Command Modes

Interface configuration mode (config-interface-*interface-name*)

Command History

Release	Modification
Cisco Catalyst SD-WAN Manager Release 20.16.1	This command was introduced.

Example

```
Device(config)# sdwan
Device(config-sdwan)# interface GigabitEthernet1
Device(config-interface-GigabitEthernet1)# bandwidth-upstream 300000000
```

Related Commands

Command	Description
bandwidth-downstream	Generates notifications when the bandwidth of traffic received on a physical interface exceeds 85% of the configured bandwidth reference value.

carrier

To associate a carrier name or private network identifier with a tunnel interface, use the **carrier**

command in tunnel interface configuration mode. To remove the association, use the **no** form of the command.

carrier *carrier-name*

no carrier

Syntax Description

carrier-name	Carrier name to associate with a tunnel interface. Values: **carrier1**, **carrier2**, **carrier3**, **carrier4**, **carrier5**, **carrier6**, **carrier7**, **carrier8**, **default** Default: **default**

Command Default

The carrier name 'default' is associated with a tunnel interface.

Command Modes

tunnel interface configuration mode (config-tunnel-interface)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

Example

```
Device(config)# sdwan

Device(config-sdwan)# interface GigabitEthernet1

Device(config-interface-GigabitEthernet1)# tunnel-interface
Device(config-tunnel-interface)# carrier default
```

color

To assign a color to a WAN transport tunnel, use the **color** command in tunnel interface configuration mode. To remove the color assignment and revert to the default configuration, use the **no** form of the command.

color *color*

no color

Syntax Description

color	Identify an individual WAN transport tunnel by assigning it a color. The color is one of the TLOC parameters associated with the tunnel. On a Cisco IOS XE SD-WAN device, you can configure only one tunnel interface that has the color **default**. The colors **metro-ethernet**, **mpls**, and **private1** through **private6** are private colors. They use private addresses to connect to the remote side Cisco IOS XE SD-WAN device in a private network. You can use these colors in a public network provided that there is no NAT device between the local and remote vEdge routers. Values: **3g**, **biz-internet**, **blue**, **bronze**, **custom1**, **custom2**, **custom3**, **default**, **gold**, **green**, **lte**, **metro-ethernet**, **mpls**, **private1**, **private2**, **private3**, **private4**, **private5**, **private6**, **public-internet**, **red**, and **silver**

Command Default

The transport tunnel is assigned the color **default**

Command Modes tunnel interface configuration mode (config-tunnel-interface)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

Example

```
Device(config)# sdwan

Device(config-sdwan)# interface GigabitEthernet1

Device(config-interface-GigabitEthernet1)# tunnel-interface
Device(config-tunnel-interface)# color lte
```

encapsulation

To configure the encapsulation for a tunnel interface, use the **encapsulation** command in the tunnel interface configuration mode. To disable the encapsulation configuration, use the **no** form of the command.

encapsulation { **gre** | **ipsec** } [**weight** *number*]

no encapsulation { **gre** | **ipsec** } [**weight**]

Syntax Description

{ **gre** | **ipsec** }	Configure the encapsulation to use on the tunnel interface. This encapsulation is one of the TLOC properties associated with the tunnel, along with the IP address and the color. The default IP MTU for GRE is 1468 bytes, and for IPsec it is 1442 bytes because of the larger overhead.
weight *number*	Weight to use to balance traffic across multiple tunnels (that is, across multiple TLOCs). A higher value sends more traffic to the tunnel. You typically set the weight based on the bandwidth of the TLOC. When a Cisco IOS XE SD-WAN device has multiple TLOCs, all with the highest preference, traffic distribution is weighted according to the configured weight value. For example, if TLOC A has weight 10, and TLOC B has weight 1, and both TLOCs have the same preference value, then roughly 10 flows are sent out TLOC A for every 1 flow sent out TLOC B. Range: 1 through 255 Default: 1

Command Default Encapsulation is not configured for a tunnel interface.

Command Modes Tunnel interface configuration mode (config-tunnel-interface)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For a single tunnel, you can configure both IPsec and GRE encapsulations, by including two **encapsulation** commands. Cisco SD-WAN then creates two TLOCs for the tunnel interface. Both TLOCs have the same IP address and color, but one has IPsec encapsulation while the other has GRE encapsulation.

GRE encapsulation

```
Device(config)# sdwan

Device(config-sdwan)# interface GigabitEthernet1

Device(config-interface-GigabitEthernet1)# tunnel-interface
Device(config-tunnel-interface)# encapsulation gre weight 1
```

IPsec encapsulation

```
Device(config)# sdwan

Device(config-sdwan)# interface GigabitEthernet1

Device(config-interface-GigabitEthernet1)# tunnel-interface
Device(config-tunnel-interface)# encapsulation ipsec weight 1
```

gre-in-udp

To enable GRE-in-UDP packet encapsulation, use the **gre-in-udp** command in tunnel interface configuration mode. To disable GRE-in-UDP packet encapsulation, use the **no** form of the command.

gre-in-udp

no gre-in-udp

Command Default

gre-in-udp is not enabled.

Command Modes

tunnel interface configuration mode (config-tunnel-interface)

Table 44: Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	This command was introduced.

Usage Guidelines

Use the command **encapsulation gre** to enable GRE packet encapsulation. Then enable GRE-in-UDP packet encapsulation mode.

Example

The following example shows how to enable GRE-in-UDP.

```
device(config)# sdwan

device(config-sdwan)# interface GigabitEthernet1

device(config-interface-GigabitEthernet1)# tunnel-interface
device(config-tunnel-interface)# encapsulation gre
device(config-tunnel-interface)# gre-in-udp
```

exclude-controller-group-list

To configure Cisco vSmart Controllers with which a tunnel interface is not allowed to establish control connections, use the **exclude-controller-group-list** command in tunnel interface configuration mode. To remove the configuration, use the **no** form of the command.

exclude-controller-group-list *number*

no exclude-controller-group-list *number*

Syntax Description

number	Identifiers of one or more Cisco vSmart controller groups that this tunnel is not allowed to establish control connections with. Separate multiple numbers with a space. Range: 0 through 100

Command Default

No Cisco vSmart controller group is excluded.

Command Modes

tunnel interface configuration mode (config-tunnel-interface)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

On a system-wide basis, you configure all the Cisco vSmart controllers that the router can connect to using the **system controller-group-list** command. Use the **exclude-controller-group-list** command to restrict the Cisco vSmart controllers to which a particular tunnel interface can establish connections.

Example

```
Device(config)# sdwan

Device(config-sdwan)# interface GigabitEthernet1

Device(config-interface-GigabitEthernet1)# tunnel-interface
Device(config-tunnel-interface)# exclude-controller-group-list 1
```

hello-interval

To configure the keepalive interval between Hello packets sent on a DTLS or TLS WAN transport connection, use the **hello-interval** command in tunnel interface configuration mode. To revert to the default configuration, use the **no** form of the command.

hello-interval *milliseconds*

no hello-interval

Syntax Description

milliseconds Interval between Hello packets sent on a DTLS or TLS WAN tunnel connection. The combination of the hello interval and hello tolerance determines how long to wait before declaring a DTLS or TLS tunnel to be down.

The hello tolerance interval must be at least two times the tunnel hello interval. The default hello interval is 1000 milliseconds (1 second).

Note
The hello interval is configured in milliseconds, and the hello tolerance is configured in seconds.

With the default hello interval of 1 second and the default tolerance of 12 seconds, if no Hello packet is received within 11 seconds, the tunnel is declared down at 12 seconds. If the hello interval or the hello tolerance, or both, are different at the two ends of a DTLS or TLS tunnel, the tunnel chooses the interval and tolerance as follows:

- For a tunnel connection between a Cisco IOS XE SD-WAN device and any controller device, the tunnel uses the hello interval and tolerance times configured on the Cisco IOS XE SD-WAN device. This choice is made to minimize the amount traffic sent over the tunnel, to allow for situations where the cost of a link is a function of the amount of traffic traversing the link. The hello interval and tolerance times are chosen separately for each tunnel between a Cisco IOS XE SD-WAN device and a controller device.

Range: 100 through 600000 milliseconds (10 minutes)

Default: 1000 milliseconds (1 second)

Note
If the tunnel interface is configured as a low-bandwidth link, the control connection might flap if you use a hello-interval of 100 milliseconds. For low-bandwidth link interfaces, use hello-interval of more than 100 milliseconds.

Command Default

The default hello interval is 1000 milliseconds.

Command Modes

tunnel interface configuration mode (config-tunnel-interface)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

Example

```
Device(config)# sdwan

Device(config-sdwan)# interface GigabitEthernet1

Device(config-interface-GigabitEthernet1)# tunnel-interface
Device(config-tunnel-interface)# hello-interval 1000
```

hello-tolerance

To configure how long to wait for a Hello packet on a DTLS or TLS WAN transport connection before declaring that transport tunnel to be down, use the **hello-tolerance** command in tunnel interface configuration mode. To revert to the default configuration, use the **no** form of the command.

hello-tolerance *seconds*

no hello-tolerance

Syntax Description

seconds	How long to wait since the last Hello packet was sent on a DTLS or TLS WAN tunnel connection before declaring the tunnel to be down. The hello tolerance interval must be at least twice the hello interval, to ensure that at least one keepalive packet reaches and then returns from the remote side before timing out the peer. The default hello interval is 1000 milliseconds (1 second). **Note** The hello interval is configured in milliseconds, and the hello tolerance is configured in seconds. The combination of the hello interval and hello tolerance determines how long to wait before declaring a DTLS or TLS tunnel to be down. With the default hello interval of 1 second and the default tolerance of 12 seconds, if no Hello packet is received within 11 seconds, the tunnel is declared down at 12 seconds. If the hello interval or the hello tolerance, or both, are different at the two ends of a DTLS or TLS tunnel, the tunnel chooses the interval and tolerance as follows: • For a tunnel connection between a Cisco IOS XE SD-WAN device and any controller device, the tunnel uses the hello interval and tolerance times configured on the Cisco IOS XE SD-WAN device. This choice is made to minimize the amount traffic sent over the tunnel, to allow for situations where the cost of a link is a function of the amount of traffic traversing the link. The hello interval and tolerance times are chosen separately for each tunnel between a Cisco IOS XE SD-WAN device and a controller device. Range: 12 through 6000 seconds (10 minutes) Default: 12 seconds

Command Default

The default hello tolerance is 12 seconds.

Command Modes tunnel interface configuration mode (config-tunnel-interface)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

Example

```
Device(config)# sdwan

Device(config-sdwan)# interface GigabitEthernet1

Device(config-interface-GigabitEthernet1)# tunnel-interface
Device(config-tunnel-interface)# hello-tolerance 12
```

iperf-server

Specify a private iPerf3 server that a device contacts to perform a speed test for automatic bandwidth detection. To remove the private iPerf3 server specification, use the **no** form of this command.

iperf-server *ipv4-address*
no iperf-server

Syntax Description

ipv4-address	IPv4 address of a private iPerf3 server used for automatic bandwidth detection.

Command Default None

Command Modes SD-WAN physical interface configuration mode (config-interface-*interface-name*)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	This command was introduced.

Usage Guidelines When you use the auto-bandwidth-detect command to configure a device to perform automatic bandwidth detection, the device contacts an iPerf3 server to perform a speed test to determine the bandwidth. By default, the device contacts a public iPerf3 server for this speed test. Use the iperf-server to designate a private iPerf3 server that a device contacts instead.

We recommend that you use a private iPerf3 server. If a private iPerf3 server is not specified, the device pings a system defined set of public iPerf3 servers and selects for the speed test the public server with the minimum hops value. If all servers have the same minimum hops value, the device selects the server with the minimum and latency value. If the speed test fails, the device selects another public server from the list. The device continues to select other public iPerf3 servers until the speed test is successful or until it has tried all servers. Therefore, a speed test on a public iPerf3 server can use a server that is far away and there can be a larger latency than the minimum.

Example

The following example shows how to specify a private iPerf3 server for automatic bandwidth detection:

```
Device(config)# sdwan
Device(config-sdwan)# interface GigabitEthernet1
Device(config-interface-GigabitEthernet1) auto-bandwidth-detect
Device(config-interface-GigabitEthernet1) iperf-server 10.1.1.1
```

Table 45: Related Commands

Command	Description
auto-bandwidth-detect	Configure a device to automatically determine the bandwidth for WAN interfaces in VPN0 during day 0 onboarding by performing a speed test using an iPerf3 server.

last-resort-circuit

To configure a tunnel interface as the circuit of last resort, use the **last-resort-circuit** command in tunnel interface configuration mode. To remove the configuration as the circuit of last resort, use the **no** form of the command.

last-resort-circuit

no last-resort-circuit

Syntax Description

This command has no arguments or keywords.

Command Default

By default, this feature is disabled, and the tunnel interface is not considered to be the circuit of last resort.

Command Modes

tunnel interface configuration mode (config-tunnel-interface)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

There is a delay of 7 seconds before switching back to the primary tunnel interface from a circuit of last resort. This delay is to ensure that the primary interface is once again fully operational and is not still flapping.

When you configure a tunnel interface to be a last-resort circuit, the cellular modem becomes dormant and no traffic is sent over the circuit. However, the cellular modem is kept in online mode so that the modem radio can be monitored at all times and to allow for faster switchover in the case the tunnel interface needs to be used as the last resort.

To minimize the amount of extraneous data plane traffic on a cellular interface that is a circuit of last resort, increase the BFD Hello packet interval and disable PMTU discover.

Example

```
Device(config)# sdwan

Device(config-sdwan)# interface GigabitEthernet1

Device(config-interface-GigabitEthernet1)# tunnel-interface
Device(config-tunnel-interface)# last-resort-circuit
```

low-bandwidth-link

To configure a tunnel interface as a low bandwidth link, use the **low-bandwidth-link** command in tunnel interface configuration mode. To remove the low bandwidth link configuration, use the **no** form of the command.

low-bandwidth-link

no low-bandwidth-link

Syntax Description

This command has no arguments or keywords.

Command Default

This option is disabled by default.

Note Starting from Cisco IOS XE Catalyst SD-WAN Release 17.6.x, LTE enabled CPE is disabled by default.

Command Modes

tunnel interface configuration mode (config-tunnel-interface)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

This configuration command is relevant only for a spoke router in a hub-and-spoke deployment scenario, where the spoke has a low-bandwidth link, such as an LTE link.

The low bandwidth synchronizes all the BFD sessions and control session hello-interval on LTE WAN circuits to timeout at the same time. The periodic heartbeat messages are sent out at the same time to make optimal usage of LTE circuits radio waves or radio frequency energy to transmit and receive packets. The low bandwidth feature cannot reduce the number of hello packets to be transmitted (Tx) or received (Rx) for the sessions, but synchronizes the hello interval timeout for the sessions.

For example, if the BFD session and control connection hello-interval is 1 sec, and there is no user data traffic active on LTE circuits, then the sessions hello packets transmitted is spread across 1 sec window interval. Each session will timeout anywhere within that 1 sec interval and transmits the hello packet. This makes the LTE radio to be active almost all the time. With low bandwidth feature, all the session hello packets transmits at the same time, and leave the rest of the 1sec interval idle, makes optimal usage of LTE modem radio energy.

Note To prevent control-connection flapping when an interface is configured as a low-bandwidth link, use a hello-interval of greater than 100 milliseconds.

Example

```
Device(config)# sdwan

Device(config-sdwan)# interface GigabitEthernet1

Device(config-interface-GigabitEthernet1)# tunnel-interface
Device(config-tunnel-interface)# low-bandwidth-link
```

max-control-connections

To configure the maximum number of Cisco Catalyst SD-WAN Controllers that a Cisco IOS XE Catalyst SD-WAN device is allowed to connect to, use the **max-control-connections** command in tunnel interface configuration mode. To remove the configuration, use the **no** form of the command.

Note For control connection traffic without dropping any data, a minimum of 650-700 kbps bandwidth is recommended with default parameters configured for hello-interval (10) and hello-tolerance (12).

max-control-connections *number*

no max-control-connections

Syntax Description

number	Sets the maximum number of Cisco Catalyst SD-WAN Controllers that the vEdge router can connect to. These connections are DTLS or TLS control plane tunnels. Range: 0 through 100 Default:

Command Default

By default, the maximum number of controller connections is set to the same value as the maximum number of OMP sessions configured using the **system max-omp-sessions** command.

Command Modes

tunnel interface configuration mode (config-tunnel-interface)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

When **max-control-connections** is configured without affinity, devices establish control connection with Cisco Catalyst SD-WAN Controllers having higher System-IP.

Example

```
Device(config)# sdwan

Device(config-sdwan)# interface GigabitEthernet1

Device(config-interface-GigabitEthernet1)# tunnel-interface
Device(config-tunnel-interface)# max-control-connections 1
```

nat-refresh-interval

To configure the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection, use the **nat-refresh-interval** command in tunnel interface configuration mode. This interval is how often a tunnel interface sends a refresh packet to maintain the UDP packet streams that traverse a NAT. To revert to the default configuration, use the **no** form of the command.

nat-refresh-interval *seconds*

no nat-refresh-interval

Syntax Description

seconds	Interval between NAT refresh packets sent on a DTLS or TLS WAN tunnel connection. These packets are sent to maintain the UDP packet streams that traverse a NAT between the device and the Internet or other public network. You might want to increase the interval on interfaces where you are charged for bandwidth, such as LTE interfaces. Range: 1 through 60 seconds Default: 5 seconds

Command Default

A tunnel interface has a default NAT refresh interval of 5 seconds.

Command Modes

tunnel interface configuration mode (config-tunnel-interface)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

Example

```
Device(config)# sdwan

Device(config-sdwan)# interface GigabitEthernet1

Device(config-interface-GigabitEthernet1)# tunnel-interface
Device(config-tunnel-interface)# nat-refresh-interval 5
```

port-hop

On a Cisco IOS XE SD-WAN device behind a NAT device, to configure a tunnel interface to rotate through a pool of preselected OMP port numbers, known as base ports, to establish DTLS connections with other WAN edge devices when a connection attempt is unsuccessful, use the **port-hop** command in tunnel interface configuration mode. To disable port hopping for a tunnel interface, use the **no** form of the command.

port-hop

no port-hop

Syntax Description

This command has no arguments or keywords.

Command Default

Port hopping is enabled on a tunnel interface.

Command Modes

tunnel interface configuration mode (config-tunnel-interface)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For a tunnel interface (TLOC) on a Cisco IOS XE SD-WAN device behind a NAT device, you can configure the interface to rotate through a pool of preselected OMP port numbers, known as base ports, to establish DTLS connections with other WAN edge devices when a connection attempt is unsuccessful. By default, port hopping is enabled on Cisco IOS XE SD-WAN devices and on all tunnel interfaces on Cisco IOS XE SD-WAN devices.

There are five base ports: 12346, 12366, 12386, 12406, and 12426. These port numbers determine the ports used for connection attempts. The first connection attempt is made on port 12346. If the first connection does not succeed after about 1 minute, port 12366 is tried. After about 2 minutes, port 12386 is tried; after about 5 minutes, port 12406; after about 6 minutes, port 12426 is tried. Then the cycle returns to port 12346.

If you have configured a port offset with the **port-offset** command, the five base ports are a function of the configured offset. For example, with a port offset of 2, the five base ports are 12348, 12368, 12388, 12408, and 12428. Cycling through these base ports happens in the same way as if you had not configured an offset.

Example

```
Device(config)# sdwan

Device(config-sdwan)# interface GigabitEthernet1

Device(config-interface-GigabitEthernet1)# tunnel-interface
Device(config-tunnel-interface)# port-hop
```

tloc-extension

To bind an interface, which connects to another WAN edge device at the same physical site, to the local device's WAN transport interface, use the **tloc-extension** command in the SD-WAN physical interface configuration mode. Note that you can configure the two devices themselves with different site identifiers. To remove the binding, use the **no** form of the command.

tloc-extension *interface-name*

no tloc-extension

Syntax Description

interface-name	Physical interface on the local router that connects to the WAN transport circuit. The interface can be a Gigabit Ethernet interface (**ge**) or a PPP interface (ppp).

Command Default

Command Modes

SD-WAN physical interface configuration mode (config-interface-*interface-name*)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

Example

```
Device(config)# sdwan

Device(config-sdwan)# interface ge0/2.101

Device(config-interface-ge0/2.101)# tloc-extension ge0/0
```

tunnel-interface

To configure an interface as a secure DTLS or TLS WAN transport connection, use the **tunnel-interface** command in the GigabitEthernet interface configuration mode. To disable the tunnel interface configuration, use the **no** form of the command.

tunnel-interface

no tunnel-interface

Syntax Description

This command has no arguments or keywords.

Command Default

A GigabitEthernet interface is not configured as a transport connection.

Command Modes

GigabitEthernet interface configuration mode (config-interface-GigabitEthernet)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

Configuring an interface to be a transport tunnel enables the flow of control and data traffic on the interface. On a Cisco IOS XE SD-WAN device, you must also configure the interface's TLOC attributes, which are carried in the TLOC OMP routes that the device sends to the Cisco vSmart controllers in its domain. For the TLOC attributes on the device, you must configure, at a minimum, a color and an encapsulation type. These two attributes, along with the router's system IP address, are the 3-tuple that uniquely identify each TLOC.

Example

```
Device(config)# sdwan

Device(config-sdwan)# interface GigabitEthernet1

Device(config-interface-GigabitEthernet1)# tunnel-interface
```

vbond-as-stun-server

To enable Session Traversal Utilities for NAT (STUN) and allow the tunnel interface to discover its public IP address and port number when the Cisco IOS XE SD-WAN device is located behind a NAT, use the **vbond-as-stun-server** command in tunnel interface configuration mode. When you configure this command, Cisco IOS XE SD-WAN devices can exchange their public IP addresses and port numbers over private TLOCs. To disable STUN, use the **no** form of the command.

vbond-as-stun-server

no vbond-as-stun-server

Syntax Description

This command has no arguments or keywords.

Command Default

STUN is not enabled by default.

Command Modes

tunnel interface configuration mode (config-tunnel-interface)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

With this configuration, the Cisco IOS XE SD-WAN device uses the Cisco vBond orchestrator as a STUN server, so that the device can determine its public IP address and public port number. The device cannot learn the type of NAT that it is behind. No overlay network control traffic is sent and no keys are exchanged over tunnel interface configured to use the Cisco vBond orchestrator as a STUN server. However, BFD does come up on the tunnel, and data traffic can be sent on it.

Example

```
Device(config)# sdwan

Device(config-sdwan)# interface GigabitEthernet1

Device(config-interface-GigabitEthernet1)# tunnel-interface
Device(config-tunnel-interface)# vbond-as-stun-server
```

vmanage-connection-preference

To configure the preference for using a tunnel interface to exchange control traffic with the Cisco vManage NMS, use the **vmanage-connection-preference** command in tunnel interface configuration mode. Configuring this option is useful for LTE and other links on which you want to minimize traffic. To remove the configured preference and revert to the default configuration, use the **no** form of the command.

vmanage-connection-preference *number*

no vmanage-connection-preference

Syntax Description

number	Preference for using the tunnel interface to exchange control traffic with the Cisco vManage NMS. The tunnel with the higher value has a greater preference to be used for connections to the Cisco vManage NMS. To have a tunnel interface never connect to the Cisco vManage NMS, set the preference value to 0. At least one tunnel interface on the Cisco IOS XE SD-WAN device must have a non-0 preference value. Range: 0 through 8 Default: 5

Command Default

A tunnel interface has a default preference of 5.

Command Modes

tunnel interface configuration mode (config-tunnel-interface)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

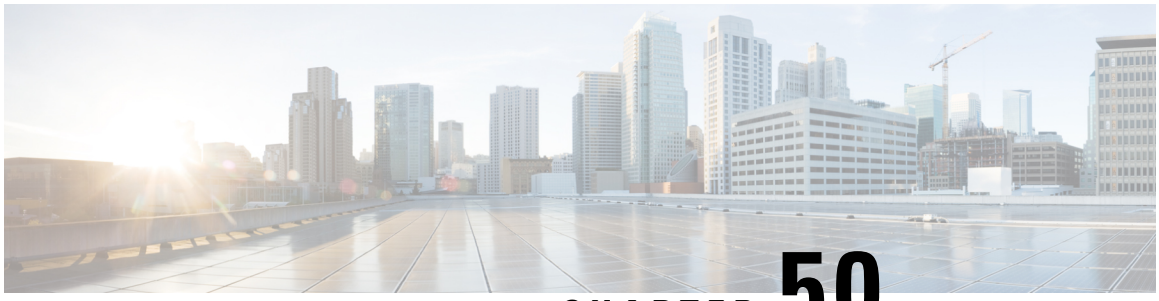
Usage Guidelines

Example

```
Device(config)# sdwan

Device(config-sdwan)# interface GigabitEthernet1

Device(config-interface-GigabitEthernet1)# tunnel-interface
Device(config-tunnel-interface)# vmanage-connection-preference 5
```



CHAPTER 50

Security Commands

- all-auto-sig-tunnels, on page 731
- authentication event fail, on page 732
- authentication event no-response action, on page 733
- authentication event server dead action authorize, on page 733
- authentication host-mode, on page 734
- aaa authentication dot1x, on page 735
- authentication open, on page 735
- authentication order, on page 736
- authentication port-control, on page 736
- authentication timer inactivity, on page 737
- authentication timer reauthenticate, on page 737
- authentication-type (security ipsec), on page 738
- dot1x pae, on page 739
- dot1x system-auth-control, on page 740
- extended-ar-window, on page 740
- ip access-group, on page 741
- ipsec (security), on page 741
- ip scp server enable, on page 742
- pairwise-keying (security ipsec), on page 743
- pwk-sym-rekey (security ipsec), on page 743
- rekey (security ipsec), on page 744
- replay-window (security ipsec), on page 744
- security, on page 745
- security ipsec integrity-type, on page 745
- sig-tunnel-list, on page 746
- switchport port-security, on page 747
- switchport port-security mac-address sticky, on page 748

all-auto-sig-tunnels

To start probe on all auto SIG active tunnels, use the **all-auto-sig-tunnels** in global configuration mode. To disable probing on all auto SIG active tunnels, use the **no** form of this command.

all-auto-sig-tunnels

no all-auto-sig-tunnels

Syntax Description This command has no arguments or keywords.

Command Modes global configuration mode

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines Use **all-auto-sig-tunnels** to enable the CXP probes in all the active auto SIG tunnels configured in the node to select the best possible SIG tunnel for accessing the SaaS applications.

Examples The following example shows how to configure probing on all active auto SIG tunnels:

```
Device(config)# probe-path branch all-auto-sig-tunnels
```

authentication event fail

To specify how the Auth Manager handles authentication failures as a result of unrecognized user credentials, use the **authentication event fail**command in interface configuration mode. To return to the default setting, use the **no** form of this command.

Supported Parameters

action	Specifies the action to be taken after an authentication failure as a result of incorrect user credentials.
authorize vlan *vlan-id*	Authorizes a restricted VLAN on a port after a failed authentication attempt.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines For more information about this command, see the Cisco IOS XE authentication event fail command.

Examples

```
interface {intf-name}
switchport mode access
switchport access vlan {vlan_id}
dot1x pae authenticator
authentication order dot1x mab
authentication host-mode single-host
authentication port-control auto
authentication timer reauthenticate <timer_num/server>
authentication timer inactivity <timer_num/server>
```

```
authentication event server dead action authorize vlan {critical_vlan}
authentication event fail action authorize vlan {restrict_vlan}
authentication event no-response action authorize vlan {guest_vlan}
no shutdown
```

authentication event no-response action

To specify how the Auth Manager handles authentication failures as a result of a nonresponsive host, use the **authentication event no-response action** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

Supported Parameters

authorize vlan *vlan-id*	Authorizes a restricted VLAN on a port after a failed authentication attempt.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE authentication event no-response action command.

```
interface {intf-name}
switchport mode access
switchport access vlan {vlan_id}
dot1x pae authenticator
authentication order dot1x mab
authentication host-mode single-host
authentication port-control auto
authentication timer reauthenticate <timer_num/server>
authentication timer inactivity <timer_num/server>
authentication event server dead action authorize vlan {critical_vlan}
authentication event fail action authorize vlan {restrict_vlan}
authentication event no-response action authorize vlan {guest_vlan}
no shutdown
```

authentication event server dead action authorize

To authorize Auth Manager sessions when the authentication, authorization, and accounting (AAA) server becomes unreachable, use the **authentication event server dead action authorize** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

Supported Parameters

vlan *vlan-id*	Authorizes a restricted VLAN on a port after a failed authentication attempt.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE authentication event server dead action authorize command.

Examples

```
interface {intf-name}
switchport mode access
switchport access vlan {vlan_id}
dot1x pae authenticator
authentication order dot1x mab
authentication host-mode single-host
authentication port-control auto
authentication timer reauthenticate <timer_num/server>
authentication timer inactivity <timer_num/server>
authentication event server dead action authorize vlan {critical_vlan}
authentication event fail action authorize vlan {restrict_vlan}
authentication event no-response action authorize vlan {guest_vlan}
no shutdown
```

authentication host-mode

To allow hosts to gain access to a controlled port, use the **authentication host-mode** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

Supported Parameters

single-host	Specifies that only one client can be authenticated on a port at any given time. A security violation occurs if more than one client is detected.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE authentication host-mode command.

Examples

```
interface {intf-name}
switchport mode access
switchport access vlan {vlan_id}
dot1x pae authenticator
authentication order dot1x mab
authentication host-mode single-host
authentication port-control auto
authentication timer reauthenticate <timer_num/server>
authentication timer inactivity <timer_num/server>
authentication event server dead action authorize vlan {critical_vlan}
authentication event fail action authorize vlan {restrict_vlan}
authentication event no-response action authorize vlan {guest_vlan}
no shutdown
```

aaa authentication dot1x

To specify one or more authentication, authorization, and accounting (AAA) methods for use on interfaces running IEEE 802.1X, use the **aaa authentication dot1x** command in global configuration mode. To disable authentication, use the **no** form of this command

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE aaa authentication dot1x command

Examples

The following example shows how to enable AAA and how to create an authentication list for 802.1X. This authentication first tries to contact a RADIUS server. If this action returns an error, the user is allowed access with no authentication:

```
Device# config-transaction
Device(config)#aaa authentication dot1x default group radius none
```

authentication open

To allow a device to have network access via an interface without going through IEEE 802.1X authentication, use the **authentication open** command in the interface configuration mode. To disable open access for the interface, use the no form of the command.

authentication open

no authentication open

Syntax Description

This command has no keywords or arguments.

Command Default

Disabled

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE authentication open command.

Examples

The following example shows how to enable network access on a device without 802.1X authentication:

```
Device# config-transaction
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# authentication open
```

authentication order

To specify the order in which the Auth Manager attempts to authenticate a client on a port, use the **authentication order** command in interface configuration mode. To return to the default authentication order, use the **no** form of this command.

Supported Parameters

dot1x	Specifies IEEE 802.1X authentication.
mab	Specifies MAC-based authentication(MAB).

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE authentication order command.

authentication port-control

To configure the authorization state of a controlled port, use the **authentication port-control** command in interface configuration mode. To disable the port-control value, use the **no** form of this command.

Supported Parameters

auto	Enables port-based authentication and causes the port to begin in the unauthorized state, allowing only Extensible Authentication Protocol over LAN (EAPOL) frames to be sent and received through the port.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE authentication port-control command.

Examples

```
interface {intf-name}
switchport mode access
switchport access vlan {vlan_id}
dot1x pae authenticator
```

```
authentication order dot1x mab
authentication host-mode single-host
authentication port-control auto
authentication timer reauthenticate <timer_num/server>
authentication timer inactivity <timer_num/server>
authentication event server dead action authorize vlan {critical_vlan}
authentication event fail action authorize vlan {restrict_vlan}
authentication event no-response action authorize vlan {guest_vlan}
no shutdown
```

authentication timer inactivity

To configure the time after which an inactive Auth Manager session is terminated, use the **authentication timer inactivity** command in interface configuration mode. To disable the inactivity timer, use the **no** form of this command.

Supported Parameters

seconds	The period of inactivity, in seconds, allowed before an Auth Manager session is terminated and the port is unauthorized. The range is from 1 to 65535.
server	Specifies that the period of inactivity is defined by the Idle-Timeout value (RADIUS Attribute 28) on the authentication, authorization, and accounting (AAA) server.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE authentication timer inactivity command.

Examples

```
interface {intf-name}
switchport mode access
switchport access vlan {vlan_id}
dot1x pae authenticator
authentication order dot1x mab
authentication host-mode single-host
authentication port-control auto
authentication timer reauthenticate <timer_num/server>
authentication timer inactivity <timer_num/server>
authentication event server dead action authorize vlan {critical_vlan}
authentication event fail action authorize vlan {restrict_vlan}
authentication event no-response action authorize vlan {guest_vlan}
no shutdown
```

authentication timer reauthenticate

To specify the period of time between which the Auth Manager attempts to reauthenticate authorized ports, use the **authentication timer reauthenticate** command in interface configuration or template configuration mode. To reset the reauthentication interval to the default, use the **no** form of this command.

Supported Parameters

seconds	The number of seconds between reauthentication attempts. The range is from 1 to 65535. The default is 3600.
server	Specifies that the interval between reauthentication attempts is defined by the Session-Timeout value (RADIUS Attribute 27) on the authentication, authorization, and accounting (AAA) server.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE authentication timer reauthenticate command.

Examples

```
interface {intf-name}
switchport mode access
switchport access vlan {vlan_id}
dot1x pae authenticator
authentication order dot1x mab
authentication host-mode single-host
authentication port-control auto
authentication timer reauthenticate <timer_num/server>
authentication timer inactivity <timer_num/server>
authentication event server dead action authorize vlan {critical_vlan}
authentication event fail action authorize vlan {restrict_vlan}
authentication event no-response action authorize vlan {guest_vlan}
no shutdown
```

authentication-type (security ipsec)

To configure the type of authentication on IPsec tunnel connections between routers, use the **authentication-type** command in IPsec configuration mode. To delete the authentication type, use the no form of this command.

Note This command is not supported for Cisco IOS XE Catalyst SD-WAN Release 17.6.1a and later. Starting from Cisco IOS XE Catalyst SD-WAN Release 17.6.1a, use the **security ipsecintegrity-type** command instead.

authentication-type { **ah-no-id** | **ah-sha1-hmac** | **sha1-hmac** | **none** }

no authentication-type

Syntax Description

ah-no-id	Specifies a modified version of AH-SHA1 HMAC and ESP HMAC-SHA1 that ignores the ID field in the outer IP header of the packet.
sha1-hmac	Specifies ESP HMAC-SHA1. With this authentication type, ESP encrypts the inner header, packet payload, ESP trailer, and MPLS label (if applicable).

ah-sha1-hmac	Specifies AH-SHA1 HMAC and ESP HMAC-SHA1. With the authentication type, ESP encrypts the inner header, packet payload, ESP trailer, and MPLS label (if applicable).
none	Maps to no authentication. With this authentication type, ESP encrypts the inner header, packet payload, ESP trailer, and MPLS label (if applicable), but no HMAC-SHA1 hash is calculated.

Command Modes

IPsec configuration (config-ipsec)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	This command is no longer supported. From Cisco IOS XE Catalyst SD-WAN Release 17.6.1a, use the **security ipsec integrity-type** command instead.

Examples

The following example shows how the router negotiates with the IPsec tunnel authentication types, AH-SHA1-HMAC, SHA1-HMAC, and AH-NO-ID:

```
Router(config)# security
Router(config-security)# ipsec
Router(config-ipsec)# authentication-type sha1-hmac ah-sha1-hmac ah-no-id
```

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.

Supported Parameters

authenticator	(Optional) The interface acts only as an authenticator and will not respond to any messages meant for a supplicant.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE dot1x pae command.

Examples

```
interface {intf-name}
switchport mode access
switchport access vlan {vlan_id}
dot1x pae authenticator
authentication order dot1x mab
authentication host-mode single-host
```

```
authentication port-control auto
authentication timer reauthenticate <timer_num/server>
authentication timer inactivity <timer_num/server>
authentication event server dead action authorize vlan {critical_vlan}
authentication event fail action authorize vlan {restrict_vlan}
authentication event no-response action authorize vlan {guest_vlan}
no shutdown
```

dot1x system-auth-control

To globally enable 802.1X SystemAuthControl (port-based authentication), use the **dot1x system-auth-control**command in global configuration mode. To disable SystemAuthControl, use the **no** form of this command.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE dot1x system-auth-control command

Examples

The following example shows how to enable SystemAuthControl:

```
Device(config)# dot1x system-auth-control
```

extended-ar-window

To configure an extended anti-replay window, use the **extended-ar-window** command in the IPsec configuration mode. To remove the extended anti-replay window, use the **no** form of the command.

extended-ar-window *duration*

no extended-ar-window

Syntax Description

duration	Duration of the extended anti-replay window. Choose an appropriate duration based on the configured queue limits and the traffic profile. Default: 256 ms Range: 10ms to 2048ms

Command Default

By default, the extended anti-replay window is not configured.

Command Modes

IPsec configuration mode (config-ipsec)

Command History

Release	Modification
Cisco IOS XE Release 17.6.1a	Command introduced.

Example

In the following example, an extended anti-replay window of 256ms is configured:

```
security
 ipsec
  extended-ar-window 256
```

ip access-group

To apply an IP access list to an interface or a service policy map, use the **ip access-group** command in the appropriate configuration mode. To remove an IP access list, use the **no** form of this command.

Supported Parameters

access-list-name	Name of the existing IP access list as specified by an **ip access-list** command.
access-list-number	Number of the existing access list. • Integer from 1 to 199 for a standard or extended IP access list. • Integer from 1300 to 2699 for a standard or extended IP expanded access list.
out	Filters on outbound packets.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE ip access-group command.

Examples

```
ip access-group 1 out
ipv6 enable
keepalive 60
```

ipsec (security)

To configure the parameters for IPsec tunnel connections on routers, use the **ipsec** command in security configuration mode.

ipsec

Syntax Description

This command has no arguments or keywords.

Command Modes

security configuration (config-security)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Examples

The following example shows how to apply the IPsec rekeying interval, modify the size of IPsec replay window, and configure multiple authentication types:

```
Router(config)# security
Router(config-security)# ipsec
Router(config-ipsec)# rekey 1209600
Router(config-ipsec)# replay-window 4096
Router(config-ipsec)# authentication-type ah-sha1-hmac ah-sha1-hmac ah-no-id
Router(config-ipsec)# pairwise-keying
```

ip scp server enable

To enable the router to securely copy files from a remote workstation, use the **ip scp server enable** command in global configuration mode. To disable secure copy functionality (the default), use the **no** form of this command.

ip scp server enable
no ip scp server enable

Syntax Description

This command has no arguments or keywords.

Command Default

The secure copy function is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE ip scp server enable command.

Examples

The following example shows how to configure the router to allow the router to securely copy files from a remote workstation. AAA must be configured as scp relies on AAA authentication and authorization.

```
aaa new-model
aaa authentication login default tac-group tacacs+
aaa authorization exec default local
```

```
username user1 privilege 15 password 0 lab
ip scp server enable
```

Related Commands

Command	Description
aaa authentication login	Sets AAA authentication at login.
aaa authorization	Sets parameters that restrict user access to a network.
username	Establishes a username-based authentication system.

pairwise-keying (security ipsec)

To configure the private pairwise IPsec session keys for secure communication between IPsec routers and its peers, use the **pairwise-keying** command in IPsec configuration mode. To delete the pairwise IPsec session keys, use the no form of this command.

pairwise-keying

no pairwise-keying

Syntax Description

This command has no arguments or keywords.

Command Modes

IPsec configuration (config-ipsec)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Examples

The following example shows how to configure a pair of IPsec session keys per pair of local and remote TLOC:

```
Router(config)# security
Router(config-security)# ipsec
Router(config-ipsec)# authentication-type ah-sha1-hmac ah-sha1-hmac ah-no-id
Router(config-ipsec)# pairwise-keying
```

pwk-sym-rekey (security ipsec)

To enable symmetric rekeying when pairwise keying is enabled, use the **pwk-sym-rekey** in IPsec configuration mode. To disable symmetric rekeying, use the no form of this command.

pwk-sym-rekey

no pwk-sym-rekey

Syntax Description This command has no arguments or keywords.

Command Modes IPsec configuration (config-ipsec)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Examples The following example shows how to configure rekeying for IPsec pairwise keys:

```
Router(config)# security
Router(config-security)# ipsec
Router(config-ipsec)# pairwise-keying
Router(config-ipsec)# pwk-sym-rekey
```

rekey (security ipsec)

To modify the IPsec rekeying timer on routers, use the **rekey** command in IPsec configuration mode. To delete the rekey timer on routers, use the no form of this command.

rekey *time-interval*

no rekey

Syntax Description

time-interval	Specifies how often IKE changes the AES key that is used during IKE key exchanges. Range: 10 - 1209600 seconds (up to 14 days) Default: 86400 seconds

Command Modes IPsec configuration (config-ipsec)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Examples The following example shows how to change the rekeying interval for IKE key exchanges to 7 days:

```
Router(config)# security
Router(config-security)# ipsec
Router(config-ipsec)# rekey 604800
```

replay-window (security ipsec)

To modify the size of the IPsec replay window on routers, use the **replay-window** command in IPsec configuration mode. To delete the replay window size on routers, use the no form of this command.

replay-window *replay-window-size*

no replay-window

Syntax Description

replay-window-size	Specifies the size of the sliding replay window method. Values: 64, 128, 256, 512, 1024, 2048, 4096, 8192 packets Default: 512 packets

Command Modes

IPsec configuration (config-ipsec)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Examples

The following example changes the replay window size to 1024:

```
Router(config)# security
Router(config-security)# ipsec
Router(config-ipsec)# replay-window 1024
```

security

To configure security parameters on routers, Cisco vManage, and Cisco vSmart Controllers, use the **security** command in global configuration mode.

security

Syntax Description

This command has no arguments or keywords.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Examples

The following example shows how to configure the security for a router.

```
Router(config)# security
```

security ipsec integrity-type

To configure the type of integrity check performed on IPSec packets, use the **security ipsec integrity-type** command in global configuration mode. To delete the authentication type, use the **no** form of this command.

security ipsec integrity-type { **none** | **ip-udp-esp** | **ip-udp-esp-no-id** | **esp** }

no security ipsec integrity-type

Syntax Description

none	This option turns integrity checking off on IPSec packets. We don't recommend using this option.
ip-udp-esp	Enables ESP encryption. In addition to the integrity checks on the Encapsulating Security Payload (ESP) header and payload, the checks also include the outer IP and UDP headers.
ip-udp-esp-no-id	This is similar to ip-udp-esp option, however, the ID field of the outer IP header is ignored. Configure this option in the list of integrity types to have the Cisco SD-WAN software ignore the ID field in the IP header so that the Cisco SD-WAN can work in conjunction with non-Cisco devices.
esp	Enables ESP encryption and integrity checking on ESP header.

Command Default

When an integrity-type is not specified, tbe default integrity-type is ip-udp-esp esp.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	This command was introduced. **Note** From Cisco IOS XE Catalyst SD-WAN Release 17.6.1a, this command replaces the **security ipsec authentication-type** command.

Usage Guidelines

Configure each integrity type separately using the **security ipsec integrity-type** command.

Example

This example shows how to configure the various integrity types that are supported.

```
Device(config)# security ipsec integrity-type ip-udp-esp
Device(config)# security ipsec integrity-type ip-udp-esp-no-id
Device(config)# security ipsec integrity-type esp
```

sig-tunnel-list

To configure the manual tunnels or a specific set of auto-tunnels for probing instead of all the auto-tunnels, use the **sig-tunnel-list** command in global configuration mode.

sig-tunnel-list *list of SIG tunnels*

no probe-path gateway sig-tunnel-list

Syntax Description

list of SIG tunnels	Specifies a specific set of auto-tunnels for probing.

Command Modes

global configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Examples

The following example shows how to configure the manual tunnels or a specific set of auto-tunnels for probing instead of all the auto-tunnels:

```
Device(config)# probe-path branch sig-tunnel-list Tunnel100015 Tunnel100016
```

switchport port-security

To enable port security on an interface, use the **switchport port-security** command in interface configuration mode. To disable port security, use the **no** form of this command.

switchport port-security
no switchport port-security

Syntax Description

This command has no keywords or arguments.

Command Default

Disabled

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE switchport port-security command.

Port security configuration is supported on Cisco ISR4000 and Cisco C8300 series Edge platforms with SM-X-16G4M2X, and SM-X-40G8M2X switching modules.

Examples

The following example shows how to enable port security:

```
Device(config-if)# switchport port-security
```

The following example shows how to disable port security:

```
Device(config-if)# no switchport port-security
```

switchport port-security mac-address sticky

To configure the dynamic MAC addresses as sticky on an interface, use the **switchport port-security mac-address sticky** command. To disable the sticky feature on an interface, use the **no** form of this command.

switchport port-security mac-address sticky
no switchport port-security mac-address sticky

Syntax Description

sticky	Configures the dynamic MAC addresses as sticky on an interface. By default, sticky is disabled.

Command Default

MAC addresses are not classified as secured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE switchport port-security mac-address command.

Port security configuration is supported on Cisco ISR4000 and Cisco C8300 series Edge platforms with SM-X-16G4M2X, and SM-X-40G8M2X switching modules.

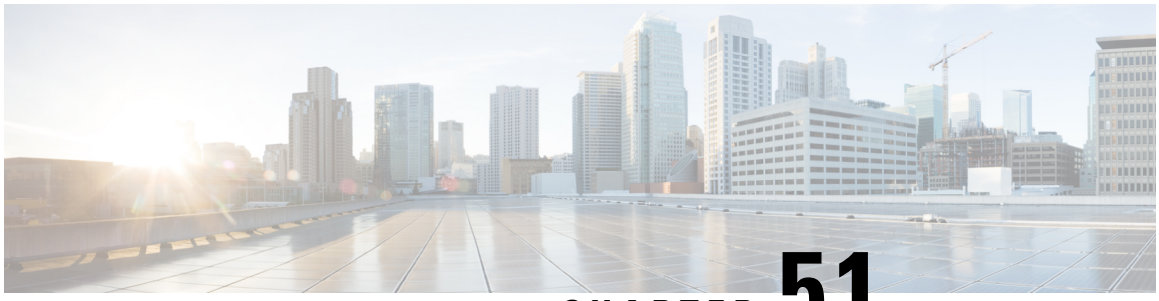
Examples

The following example shows how to enable the sticky feature on an interface:

```
Device(config-if)# switchport port-security mac-address sticky
```

The following example shows how to disable the sticky feature on an interface:

```
Device(config-if)# no switchport port-security mac-address sticky
```



CHAPTER 51

Service Insertion Commands

- service-chain, on page 749
- service-chain-affect-bfd, on page 750
- service-chain-description, on page 751
- service-chain-enable, on page 752
- service-chain-vrf, on page 753
- service, on page 755
- service service-transport-ha-pair attribute trust-posture, on page 758
- track-enable, on page 759

service-chain

To create a service chain, use the **service-chain** command in SD-WAN configuration mode. To remove a service chain, use the **no** form of the command.

service-chain *chain-number*

no service-chain *chain-number*

Syntax Description

chain-number	Identifier of the service chain. Valid values: SC1 through SC16.

Command Default

A service chain is not created.

Command Modes

SD-WAN configuration (config-sdwan)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.13.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

You can create up to 16 service chains in a Cisco Catalyst SD-WAN network.

Example

The following example shows how to create a service chain named SC1:

```
Device(config)# sdwan
Device(config-sdwan)# service-chain SC1
```

Related Commands

Command	Description
service	Specifies the services that are in the service chain.
service service-transport-ha-pair attribute trust-posture	Specifies the trust posture for a high availability pair that is in a service chain
service-chain-affect-bfd	Configures all Cisco Catalyst SD-WAN bidirectional forwarding sessions to be brought down automatically and immediately if the service chain goes down
service-chain-description	Configures a description for a service chain
service-chain-enable	Enables a service chain, which makes it active on devices.
service-chain-vrf	Specifies the name of the VPN in which all services in the service chain are to be hosted.
track-enable	Specifies that the IP address of each service in the service chain can be tracked by using endpoint tracking.

service-chain-affect-bfd

To configure all Cisco Catalyst SD-WAN bidirectional forwarding (BFD) sessions to be brought down automatically and immediately if the service chain goes down, use the **service-chain-affect-bfd** command in service-chain configuration mode. To remove this configuration, use the **no** form of this command.

service-chain-affect-bfd

no service-chain-affect-bfd

Syntax Description

This command has no arguments or keywords.

Command Default

Cisco Catalyst SD-WAN BFD sessions are not brought down automatically if the service chain goes down.

Command Modes

service-chain configuration (config-service-chain)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.13.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

- This command is available after you create a service chain with the **service-chain** command.
- Unless you require all BFD sessions to be brought down when a service chain goes down, we recommend that this command not be used to prevent the unintended disruption of BFD.

Example

The following example shows how to enable Cisco Catalyst SD-WAN BFD sessions to be brought down automatically and immediately if the service chain SC1 goes down:

```
Device(config)# sdwan
Device(config-sdwan)# service-chain SC1
Device(config-service-chain-SC1)# service-chain-affect-bfd
```

Related Commands

Command	Description
service-chain	Creates a service chain.
service-chain-description	Configures a description for a service chain
service-chain-enable	Enables a service chain, which makes it active on devices.
service-chain-vrf	Specifies the name of the VPN in which all services in the service chain are to be hosted.
service	Specifies the services that are in the service chain.
service service-transport-ha-pair attribute trust-posture	Specifies the trust posture for a high availability pair that is in a service chain
track-enable	Specifies that the IP address of each service in the service chain can be tracked by using endpoint tracking.

service-chain-description

To configure a description for a service chain, use the **service-chain-description** command in service-chain configuration mode. To remove the description from a service chain, use the **no** form of this command.

service-chain-description *description*

no service-chain-description

Syntax Description

description	Description of the service chain. The description can contain up to 64 characters.

Command Default

A description for the service chain is not configured.

Command Modes

service-chain configuration (config-service-chain)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.13.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

This command is available after you create a service chain with the **service-chain** command.

Example

The following example shows how to configure "service-chain-site-1" as the description of service chain SC1:

```
Device(config)# sdwan
Device(config-sdwan)# service-chain SC1
Device(config-service-chain-SC1)# service-chain-description service-chain-site-1
```

Related Commands

Command	Description
service-chain	Creates a service chain.
service-chain-affect-bfd	Configures all Cisco Catalyst SD-WAN bidirectional forwarding sessions to be brought down automatically and immediately if the service chain goes down
service-chain-enable	Enables a service chain, which makes it active on devices.
service-chain-vrf	Specifies the name of the VPN in which all services in the service chain are to be hosted.
service	Specifies the services that are in the service chain.
service service-transport-ha-pair attribute trust-posture	Specifies the trust posture for a high availability pair that is in a service chain
track-enable	Specifies that the IP address of each service in the service chain can be tracked by using endpoint tracking.

service-chain-enable

To enable a service chain, which makes it active on devices, use the **service-chain-enable** command in service-chain configuration mode. To disable the service chain, use the **no** form of this command.

service-chain-enable

no service-chain-enable

Syntax Description

This command has no arguments or keywords.

Command Default

A service chain is enabled.

Command Modes service-chain configuration (config-service-chain)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.13.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

- This command is available after you create a service chain with the **service-chain** command.
- Because a service chain is enabled by default, you do not need to use this command to enable s service chain unless you have first used this command to disable the service chain.
- This command is useful when you want to create a service chain but are not ready for it to become active. In this situation, create the service chain and use this command disable it. You enable the service chain later when you want it to be active.

Example

The following example shows how to enable service chain SC1:

```
Device(config)# sdwan
Device(config-sdwan)# service-chain SC1
Device(config-service-chain-SC1)# service-chain-enable
```

Related Commands

Command	Description
service-chain	Creates a service chain.
service-chain-affect-bfd	Configures all Cisco Catalyst SD-WAN bidirectional forwarding sessions to be brought down automatically and immediately if the service chain goes down
service-chain-description	Configures a description for a service chain
service-chain-vrf	Specifies the name of the VPN in which all services in the service chain are to be hosted.
service	Specifies the services that are in the service chain.
service service-transport-ha-pair attribute trust-posture	Specifies the trust posture for a high availability pair that is in a service chain
track-enable	Specifies that the IP address of each service in the service chain can be tracked by using endpoint tracking.

service-chain-vrf

To specify the name of the VPN that hosts all services in the service chain, use the **service-chain-vrf** command in service-chain configuration mode.

service-chain-vrf *vrf*

Syntax Description

vrf	Name of a configured VPN in which all services in the service chain are to be hosted.

Command Default

A VRF name is not specified.

Command Modes

service-chain configuration (config-service-chain)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.13.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

- This command is available after you create a service chain with the **service-chain** command.
- All services in the service chain must be accessible through the VPN that you specify.
- This command does not have a **no** form.

Example

The following example shows how to specify 101 as the VPN in which all services in the service chain SC1 are to be hosted:

```
Device(config)# sdwan
Device(config-sdwan)# service-chain SC1
Device(config-service-chain-SC1)# service-chain-vrf 101
```

Related Commands

Command	Description
service-chain	Creates a service chain.
service-chain-affect-bfd	Configures all Cisco Catalyst SD-WAN bidirectional forwarding sessions to be brought down automatically and immediately if the service chain goes down
service-chain-description	Configures a description for a service chain
service-chain-enable	Enables a service chain, which makes it active on devices.
service	Specifies the services that are in the service chain.
service service-transport-ha-pair attribute trust-posture	Specifies the trust posture for a high availability pair that is in a service chain
track-enable	Specifies that the IP address of each service in the service chain can be tracked by using endpoint tracking.

service

To specify the services that are in the service chain and configure related options, use the **service** command in service-chain configuration mode. To remove a service from a service chain, use the **no** form of this command

service *service-type service-parameters*

no service *service-type*

Syntax Description

service-type	Description of a service type to include in the service chain. Enter up to four of the following description types. These descriptions are for your reference only and you can use any description for any service type. The netscv1 through netscv10 descriptions are provided for use with your own services or when you do not want to explicitly describe a service such as a firewall for security reasons. • **firewall** • **intrusion-detection** • **intrusion-detection-prevention** • **netscv1** through **netsvc10**
service-parameters	Parameters for each service type. See Usage Guidelines for information about applicable service parameters.

Command Default

A service chain is not configured.

Command Modes

service-chain configuration (config-service-chain)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.13.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

- This command is available after you specify the name of the VPN in which all services in the service chain are to be hosted with the **service-chain-vrf** command.
- A service chain must have at least one service, so you cannot remove all services from a service chain.
- Using a *service-type* name that corresponds to a service provides a convenient way for you to identify a service in a service chain. However, any service can be connected to any *service-type* name.
- Configure the following *service-parameters* for each service type:
  - **sequence** *sequence-number*

Relative position of the service type in the service chain, which is the order in which the services in the service chain are applied to traffic. Services are applied from the lowest *sequence-number* value to the highest, and this value can be any number from 1 through 65535.

We recommend that you leave gaps between *sequence-number* values so that you can easily add services to a service chain if needed. For example, if you create a service chain with two service types, assign the service types sequence numbers of 100 and 200. The service type with a *sequence-number* of 100 is applied to traffic first. If you then want add a third sequence but want it to be applied in the second position, you can assign it a sequence number of 150 (or any value between 100 and 200).

- **service-transport-ha-pair** *value* {**active** | [**backup**]} {**tx** | [**rx**]} {{**ipv4** | **ipv6** | **tunnel-interface**} *address-or-number*} {*interface port-number interface-name*} [**endpoint-tracker** *name*]

  Specifies the number of high availability pairs (active and optionally backup interfaces) that can be configured for forwarding traffic for the service and configures these high availability pairs.

  value is the number of high availability pairs and can be a number 1 through 8. The high availability pairs can use IPv4, IPv6, or tunneled interfaces, depending on how the service is attached to a router. For dual stack connectivity, configure up to four IPv4 and four IPv6 high availability pairs.

  active specifies an active interface, and **backup** specifies a backup interface.

  tx specifies that packets are sent on the interface, and **rx** specifies that packets are received on the interface. If **rx** is not specified, packets are both sent and received on the interface.

  ipv4, **ipv6**, or **tunnel-interface** specify the method by which the service is attached to a router.

  For the IPv4 or IPv6 attachment method *address-or-number*is the IP address of the service to be attached to the service type. For the tunnel interface attachment method, *address-or-number* is the tunnel number for the service to be attached to the service type.

  interface is the type of interface that is used to connect to the service, *port-number* is the number of the port on which the service communicates, and *interface-name* is the name of the interface. *interface* can be any of the following:

  - **Ethernet**
  - **FastEthernet**
  - **FiveGigabitEthernet**
  - **FortyGigabitEthernet**
  - **GigabitEthernet**
  - **HundredGigabitEthernet**
  - **TenGigabitEthernet**
  - **TwentyFiveGigE**
  - **TwoGigabitEthernet**

- **endpoint-tracker** *name*

  By default, tracking is enabled for the service chain, and the tracker uses the tx and rx IP addresses of a service to track the service. Use this **endpoint-tracker** option if you want to track the service using other IP addresses. *name* is the name of the tracker that defines the IP address to use. You

can configure an endpoint tracker for the tx interface, the rx interface, or both interfaces. If you use this option, ensure that routing for this tracker is configured appropriately in your deployment.

Note For any interface, reachability for only one IPv4 address and one IPv6 address can be tracked. For example, if a high availability pair is configured with the service IP address of 10.1.1.1 on the GigabitEthernet3 interface, another service IP address cannot be tracked on GigabitEthernet3. Similarly, only one IPv4 address and one IPv6 address can be tracked for a dual stack interface.

Example

The following example shows how to configure the firewall and netsvc1 service types for service chain SC1:

```
Device(config)# sdwan
Device(config-sdwan)# service-chain SC1
Device(config-sdwan)# service-chain-vrf 101
Device(config-service-chain-SC1)# service firewall
Device(config-service-firewall)# sequence 100
Device(config-service-firewall)# service-transport-ha-pair 1
Device(config-service-transport-ha-pair-1)# active tx ipv4 10.0.0.1 GagabitEthernet 1
endpoint-tracker tracker 1
Device(config-service-transport-ha-pair-1)# service netsvc1
Device(config-service-netsvc1)# sequence 200
Device(config-service-netsvc1)# service-transport-ha-pair 1
Device(config-service-transport-ha-pair-1)# active tx ipv4 10.0.0.2 GagabitEthernet 4
```

Related Commands

Command	Description
service-chain	Creates a service chain.
service-chain-affect-bfd	Configures all Cisco Catalyst SD-WAN bidirectional forwarding sessions to be brought down automatically and immediately if the service chain goes down
service-chain-description	Configures a description for a service chain
service-chain-enable	Enables a service chain, which makes it active on devices.
service-chain-vrf	Specifies the name of the VPN in which all services in the service chain are to be hosted.
service service-transport-ha-pair attribute trust-posture	Specifies the trust posture for a high availability pair that is in a service chain
track-enable	Specifies that the IP address of each service in the service chain can be tracked by using endpoint tracking.

service service-transport-ha-pair attribute trust-posture

To configure the trust posture a high availability pair that is in a service chain, use the **service service-transport-ha-pair attribute trust-posture** command in service-chain configuration mode. To set the trust posture to trusted if it has been set to untrusted, use the **no** form of this command.

service *service-type* **service-transport-ha-pair** *value* **attribute trust-posture** { **trusted** | **untrusted** }

no attribute trust-posture

Syntax Description

service-type	Type of service for which to configure the trust posture. Enter one of the following values: • **firewall** • **intrusion-detection** • **intrusion-detection-prevention** • **netscv1** through **netsvc10**
value	The number of high availability pairs for which to configure the trust posture. Range: 1 through 8
trusted	Configures the trust posture as trusted.
untrusted	Configures the trust posture as untrusted.

Command Default

The trust posture for each interface in each high availability pair is trusted.

Command Modes

service-chain configuration (config-service-chain)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.14.1a	Command qualified for use in Cisco Catalyst SD-WAN Manager CLI templates.

Usage Guidelines

- The **service** command must be configured before you can configure a trust posture with this command. See service.
- The trust posture configuration of each high availability pair in a service chain must be the same. By default, the trust posture for each interface in each high availability pair is trusted. However, if one interface in a high availability pair has a trust posture of trusted and the other interface has a trust posture of untrusted, all high availability pairs in the service chain must be configured in this way.

Example

The following example shows how to configure the trust posture of each high availability pair in SC1 as trusted:

```
Device(config)# sdwan
Device(config-sdwan)# service-chain SC1
Device(config-sdwan)# service-chain-vrf 101
Device(config-service-chain-SC1)# service firewall
Device(config-service-firewall)# sequence 100
Device(config-service-firewall)# service-transport-ha-pair 1
Device(config-service-transport-ha-pair-1)# attribute trust-posture trusted
```

0

Related Commands

Command	Description
service-chain	Creates a service chain.
service-chain-affect-bfd	Configures all Cisco Catalyst SD-WAN bidirectional forwarding sessions to be brought down automatically and immediately if the service chain goes down
service-chain-description	Configures a description for a service chain
service-chain-enable	Enables a service chain, which makes it active on devices.
service-chain-vrf	Specifies the name of the VPN in which all services in the service chain are to be hosted.
service	Specifies the services that are in the service chain.
track-enable	Specifies that the IP address of each service in the service chain can be tracked by using endpoint tracking.

track-enable

To specify that the IP address of each service in the service chain can be tracked by using endpoint tracking, use the **service-chain track-enable** command in service-chain configuration mode. To disable the use of the IP address of each service for tracking, use the **no** form of the command.

track-enable

no track-enable

Syntax Description This command has no arguments or keywords.

Command Default This command is enabled.

Command Modes service-chain configuration (config-service-chain)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.13.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

- This command is available after you create a service chain with the **service-chain** command.
- Tracking generates an alert if a service goes down. If tracking is not enabled, you can still check the state of the Cisco Catalyst SD-WAN interface where a service is deployed to determine whether the service is up or down. For instructions, see ICMP Endpoint Tracker for NAT DIA.

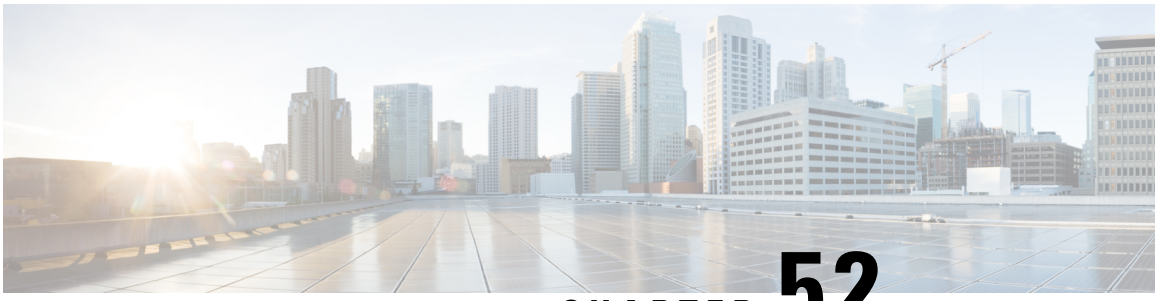
Example

The following example shows how to specify that the IP address of each service in service chain SC1 can be tracked:

```
Device(config)# sdwan
Device(config-sdwan)# service-chain SC1
Device(config-service-chain-SC1)# track-enable
```

Related Commands

Command	Description
service-chain	Creates a service chain.
service-chain-affect-bfd	Configures all Cisco Catalyst SD-WAN bidirectional forwarding sessions to be brought down automatically and immediately if the service chain goes down
service-chain-enable	Enables a service chain, which makes it active on devices.
service-chain-description	Configures a description for a service chain
service-chain-vrf	Specifies the name of the VPN in which all services in the service chain are to be hosted.
service	Specifies the services that are in the service chain.
service service-transport-ha-pair attribute trust-posture	Specifies the trust posture for a high availability pair that is in a service chain



CHAPTER 52

SHDSL Commands

- controller SHDSL, on page 761
- dsl-group, on page 762
- firmware phy filename, on page 764
- handshake, on page 765
- ignore, on page 766
- mode (SHDSL), on page 767
- shdsl annex, on page 768
- shdsl rate, on page 771
- shutdown (controller), on page 772
- termination, on page 773

controller SHDSL

To configure a controller for Single-pair High-bit-rate Digital Subscriber Line (SHDSL) mode, use the **controller SHDSL** command in global configuration mode.

controller SHDSL *slot number / subslot number / port number*

Syntax Description

slot number	Defines the slot on the router in which the high-speed WAN interface cards (HWIC) is installed.
subslot number	Defines the subslot on the router in which the HWIC is installed.
port number	Defines the port on the router in which the HWIC is installed. By default, Cisco HWIC-4SHDSL and HWIC-2SHDSL use port number 0.

Command Default

Controller number: 0

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

G.SHDSL is the technology that allows devices to send and receive high-speed symmetrical data streams over a single pair of copper wires at rates between 192 kbps and 15.36 mbps.

Example

The following example shows how to configure a SHDSL controller.

```
Device# config-t
Device(config)# controller SHDSL 0/1/0
```

dsl-group

To create and configure a digital subscriber line (DSL) group, and enter config-controller-dsl-group mode, or to automatically configure an Asynchronous Transfer Mode (ATM) group, use the **dsl-group** command in configuration controller mode. To disable the DSL group, use the **no** form of this command.

dsl-group { *dsl-group* [**pairs** | [**m-pair**]] | **auto** [**handshake** { **auto** | **g.shdsl** | **g.shdsl.bis** } | **ignore crc** { *ignore-duration* | **always** } | **shdsl** { **4-wire mode enhanced** [**vendor-id-npsg**] | **rate** { *dsl-rate* | **auto** [**current** *current-snr-margin* | **worst** *worst-snr-margin*] } } | **shutdown**] }

no dsl-group *dsl-group*

Syntax Description

dsl-group	DSL group number. The DSL group number can be one of the following: 0 to 3
pairs	Defines the DSL wire pairs.
m-pair	M-pair mode, available only in Asynchronous Transfer Mode (ATM) (configured by the **mode atm** command). When using **m-pair**, configure **pairs** to be one of the following: 0-1 0-2 0-3 2-3
efm-bond	EFM bond, available only in Ethernet in the first mile (EFM) mode (configured by the **mode efm** command).
auto	Configure the DSL group automatically.
handshake	Handshake configuration. • **auto**: Initiate auto handshake to support automatic detection of G.SHDSL or G.SHDSL.BIS. • **g.shdsl**: Support G.SHDSL. • **g.shdsl.bis**: Support G.SHDSL.BIS.

ignore crc	Ignore CRC errors. • *ignore-duration*: Amount of time (seconds) to ignore CRC errors. • **always**: Always ignore CRC errors.
shdsl	Symmetric g.shdsl configuration. See the **4-wire mode enhanced** and **rate** options below.
4-wire mode enhanced	Symmetric G.SHDSL 4-wire mode configuration. (Optional) **vendor-id-npsg**: Configure the vendor ID to NPSG.
rate	DSL line rate configuration. • *dsl-rate*: DSL rate (kbps), excluding DSL overhead. • **auto**: Auto rate mode: • **current** *current-snr-margin*: Current SNR margin (dB). • **worst** *worst-snr-margin*: Current SNR margin (dB).
shutdown	Shut down this DSL group.
no dsl-group	When using the **no** form of the command, the options depend on what has been configured.

Command Default

No DSL group is defined or automatically configured.

Command Modes

Configuration controller (config-controller)

Configuration controller DSL group (config-controller-dsl-group)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

Use the **dsl-group** command in configuration controller mode to define the DSL group, and manually configure the DSL group from configuration controller DSL group mode.

Use the **dsl-grouppairs** to define the DSL group as Ethernet First Mile (EFM) group bonding group.

Remove the DSL group before changing from a previously configured mode.

When configuring a new DSL group, configure the group with **pairs**.



Note Use the **dsl-group** command only on CPE. Do not use the Central Office (CO) option. Doing so can cause a rollback of the entire transaction.

Note Automatic configuration is not supported on IMA groups.

Automatic configuration is limited to only one DSL group and ATM interface. After a group is automatically configured, no other group can be created. All manually created groups must be deleted before creating an automatic configuration group.

```
Router(config)# controller SHDSL 0/1/0
Router(config-controller)# termination cpe
Router(config-controller)# mode atm
Router(config-controller)# dsl-group 0 pairs 0
Router(config-controller-dsl-group)#
```

```
Router(config)# controller SHDSL 0/1/0
Router(config-controller)# termination cpe
Router(config-controller)# mode atm
Router(config-controller)# dsl-group auto
Router(config-controller-dsl-group)#
```

```
Router(config)# controller SHDSL 0/1/0
Router(config-controller)# termination cpe
Router(config-controller)# mode atm
Router(config-controller)# dsl-group 0 pairs 0-3 m-pair
Router(config-controller-dsl-group)#
```

```
Router(config)# controller SHDSL 0/1/0
Router(config-controller)# termination cpe
Router(config-controller)# mode efm
Router(config-controller)# dsl-group 0 pairs 0-3 efm-bond
Router(config-controller-dsl-group)#
```

```
Router(config)# controller SHDSL 0/1/0
Router(config-controller)# termination cpe
Router(config-controller)# mode atm
Router(config-controller)# dsl-group 0 pairs 0
Router(config-controller)# dsl-group 1 pairs 2-3 m-pair
```

The following example shows how the **no** form of the command options depend on the current configuration.

```
Device(config)# controller SHDSL 0/1/0
Device(config-controller)# dsl-group 1 pairs 2-3 m-pair
Device(config-controller-dsl-group)# exit
Device(config-controller)# no dsl-group 1 pairs 2-3 m-pair
```

firmware phy filename

To perform a PHY firmware update to the Single-pair High-bit-rate Digital Subscriber Line (SHDSL) controller, use the **firmware phy filename** command in controller configuration mode.

firmware phy filename *location*

Syntax Description

location	Firmware package location, either in the router's flash memory or a USB flash drive's memory.

Command Default None

Command Modes Controller configuration (config-controller)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Example

The following example shows how to perform a PHY firmware update to SHDSL controller.

```
Device# config-t
Device(config)# controller SHDSL 0/1/0
Device(config-controller)# firmware phy filename flash:IDC_1.7.2.6_DFE_FW_BETA_120111A.pkg
```

Related Commands

Command	Description
controller SHDSL	Configures a SHDSL controller.

handshake

To configure a handshake, use the **handshake** command in the configuration controller DSL group mode. To remove handshake, use the **no** form of the command.

handshake { **auto** | **g.shdsl** | **g.shdsl.bis** | **ieee** | **itut** }

no handshake

Syntax Description

auto	Specifies automatic detection of SHDSL rates.
g.shdsl	Specifies G.SHDSL handshake.
g.shdsl.bis	Specifies G.SHDSL.BIS handshake.
ieee	Specifies IEEE handshake. This is supported in EFM mode only.
itut	Specifies ITUT handshake. This is supported in EFM mode only.

Command Default Auto

Command Modes Config controller DSL group (config-controller-dsl-group)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For better interoperability with different DSLAMs, use one of the following options with the **handshake auto** command:

- In CPE-ATM mode:
  - If DSLAM supports G.SHDSL rates, use the **g.shdsl** keyword.
  - If DSLAM supports G.SHDSL.BIS rates, use the **g.shdsl.bis** keyword.
- In EFM mode:
  - To avoid interoperability issues, use the **handshake** command with the keyword that matches the configuration that is in place during the termination at the CO.

```
Router(config)# controller SHDSL 0/1/0
Router(config-controller)# termination cpe
Router(config-controller)# mode atm
Router(config-controller)# dsl-group 0 pairs 0
Router(config-controller-dsl-group)# handshake auto
Router(config-controller-dsl-group)#

Router(config-controller-dsl-group)# no handshake
Router(config-controller-dsl-group)#
```

ignore

To ignore DSL group errors, use the **ignore** command in controller configuration DSL group mode (config-controller-dsl-grooup). To restore the default state of not ignoring errors, use the **no** form of this command.

ignore { **crc** { *seconds* | **always** } }

no ignore crc

Syntax Description

crc	Specifies cyclic redundancy check (CRC) errors.
seconds	Specifies the number of seconds to ignore errors. The range is 0 to 60 seconds.
always	Ignore errors indefinitely.

Command Default

The **no** form of this command is the default. .

Command Modes

Controller configuration DSL group mode (config-controller-dsl-grooup)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Command qualified for use in Cisco vManage CLI templates.

Examples

The following example configures a DSL group and specifies first to ignore CRC errors, then restores the default behavior of not ignoring CRC errors.

```
Router(config)# controller SHDSL 0/1/0
Router(config-controller)# termination cpe
Router(config-controller)# mode atm
Router(config-controller)# dsl-group 0 pairs 0
Router(config-controller-dsl-group)# shdsl rate auto
Router(config-controller-dsl-group)# ignore crc always
Router(config-controller-dsl-group)# no ignore crc
```

mode (SHDSL)

To set the Single-pair High-bit-rate Digital Subscriber Line (SHDSL) controller mode, use the **mode** command in controller configuration mode.

mode { **atm** | **efm** }

Syntax Description

atm	Selects the ATM (Asynchronous Transfer Mode) mode. NIM supports maximum throughput of 22.7 mbps; each line supports 5704 kbps. You can configure the lines to use 2-wire, 4-wire (standard or enhanced), or m-pair.
efm	Selects the EFM (Ethernet in the First Mile) mode. NIM supports maximum throughput of 61216 kbps; each line supports maximum of 15304 kbps with 128-TCPAM. You can configure a DSL group with any one of the lines in 2-wire nonbonding mode or with multiple lines in bonding mode.

Command Default

ATM mode

Command Modes

Controller configuration (config-controller)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

When a DSL controller is configured in ATM mode, the mode must be configured identically on both the CO and CPE sides. Both sides must be set to ATM mode.

Example

The following example shows how to select EFM mode for SHDSL controller.

```
Device# config-t
Device(config)# controller SHDSL 0/1/0
Device(config-controller)# mode efm
```

```
Device(config)# controller SHDSL 0/1/0
Device(config-controller)# termination cpe
Device(config-controller)# mode atm
Device(config-controller)# dsl-group 0 pairs 0
Device(config-controller-dsl-group)#
```

shdsl annex

To define the single-pair high-bit-rate digital subscriber line (SHDSL) G.991.2 standard, use the **shdsl annex** command in config controller DSL group mode.

shdsl annex *standard*

Syntax Description

standard	Defines the standard for the selected type of DSL group. The following annex standards are supported: • A • A-F • B (Default annexure) • B-G • F • G **IMA Group** • A • A-B • B **M-PAIR Group** • A • A-B • B • F {coding 16 | 32} • F-G {coding 16 | 32} • G {coding 16 | 32} **1-PAIR and 2-PAIR Group** • A • A-B • B • F {coding 16 | 32} • F-G {coding 16 | 32} • G {coding 16 | 32}

Command Default

SHDSL annex B

Command Modes

Config controller DSL group

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

Use the dsl-group command to create a DSL group, and then use the shdsl annex command to define the G.991.2 standard for the DSL group.

For additional usage guidelines, see the Cisco IOS XE shdsl annex command.

When using this command oin a CLI template in Cisco SD-WAN Manager, always create or delete annex together with rate. Both should be created or together in the same transaction. To delete annex, use **no shdsl annex** at the router prompt or in a CLI template. Failing to do so can cause issues in Cisco IOS, and can cause the Cisco Catalyst SD-WAN configuration to go out of synchronization with the device.

Examples

The following example uses the shdsl annex command to define the annex standard for a 2-Pair DSL group on a Cisco HWIC-4SHDSL:

```
Router(config-controller-dsl-group)# shdsl annex ?
  A    Annex A of G.991.2 standard
  A-B  Annex A/B of G.991.2 standard
  B    Annex B of G.991.2 standard
  F    Annex F of G.991.2 standard
  F-G  Annex F/G of G.991.2 standard
  G    Annex G of G.991.2 standard
Router(config-controller-dsl-group)# shdsl annex g ?
  coding  16-TCPAM or 32-TCPAM line coding
Router(config-controller-dsl-group)# shdsl annex g coding ?
  16-TCPAM  16-TCPAM line coding
  32-TCPAM  32-TCPAM line coding
Router(config-controller-dsl-group)# shdsl annex g coding 16 ?
  <cr>
```

Example

```
Router(config-controller-dsl-group)#shdsl annex ?
  A        Annex A of G.991.2 standard
  A-B-F-G  Annex A/B/F/G of G.991.2 standard
  A-F      Annex A/F of G.991.2 standard
  B        Annex B of G.991.2 standard
  B-G      Annex B/G of G.991.2 standard
  F        Annex F of G.991.2 standard
  G        Annex G of G.991.2 standard
Router(config-controller-dsl-group)#shdsl annex f ?
coding  16-TCPAM, 32-TCPAM line coding or auto-TCPAM line coding
```

The above TCPAM configurations are valid only in case the termination is "co". In case the termination is CPE, user will see the following output

```
shdsl annex { annex standard } [ coding < tcpam >]
```

```
Router(config-controller-dsl-group)# shdsl annex ?

A Annex A of G.991.2 standard
A-F Annex A/F of G.991.2 standard
B Annex B of G.991.2 standard
B-G Annex B/G of G.991.2 standard
F Annex F of G.991.2 standard
G Annex G of G.991.2 standard
```

```
Router(config-controller-dsl-group)# shdsl annex F coding ?

128-TCPAM 128-TCPAM line coding
16-TCPAM 16-TCPAM line coding
32-TCPAM 32-TCPAM line coding
4-TCPAM 4-TCPAM line coding
64-TCPAM 64-TCPAM line coding
8-TCPAM 8-TCPAM line coding


Router(config-controller-dsl-group)# shdsl annex F coding 32-TCPAM
```

shdsl rate

To define the single-pair high-bit-rate digital subscriber line (SHDSL) rate, use the **shdsl rate** command in config-controller-dsl-group mode. To delete the rate, use the **no** form of the command.

shdsl rate { *rate* | **auto** [**current** *current-snr-margin* | **worst** *worst-snr-margin*] }

no shdsl rate

Syntax Description

rate	SHDSL rate (kbps) for the digital subscriber line (DSL) group. The range options are shown below.
	• DSL group with 1 pair
	  • Annex A & B: 192-2304 kbps
	  • Annex F & G (32 TC-PAM): 768-5696 kbps
	  • Annex F & G (16 TC-PAM): 2304-3840 kbps
	• DSL group with 2 pairs
	  • Annex A & B: 384-4608 kbps
	  • Annex F & G (32 TC-PAM): 1536-11392 kbps
	  • Annex F & G (16 TC-PAM): 4608-7680 kbps
	• DSL group with 3 pairs
	  • Annex A & B: 576-6912 kbps
	  • Annex F & G (32 TC-PAM): 2304-12288 kbps
	  • Annex F & G (16 TC-PAM): 6912-11520 kbps
	• DSL group with 4 pairs
	  • Annex A & B: 768-9216 kbps
	  • Annex F & G (32 TC-PAM): 3072-16384 kbps
	  • Annex F & G (16 TC-PAM): 9216-15360 kbps

auto	Sets the SHDSL rate to automatic mode.
current *current-snr-margin*	Current signal-to-noise (SNR) margin.
worst *worst-snr-margin*	Worst SNR margin.

Command Default

For usage guidelines, see the Cisco IOS XE shdsl rate command.

Command Modes

Config controller DSL group

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

Use the dsl-group command to create a DSL group, and then use the shdsl annex command to define the G.991.2 standard for the newly created DSL group. Define the SHDSL line rate with the shdsl rate command.

Note If you enter **shdsl rate ?** at the CLI prompt to display command help, the displayed range may be incorrect.

For usage guidelines, see the Cisco IOS XE shdsl rate command.

```
Router(config)# controller SHDSL 0/1/0
Router(config-controller)# termination cpe
Router(config-controller)# mode efm
Router(config-controller)# dsl-group 0 pairs 0
Router(config-controller-dsl-group)# shdsl rate 2
Router(config-controller-dsl-group)#
```

shutdown (controller)

To shut down a DSL group, use the **shutdown** command in controller configuration mode. To reactivate the DSL group, use the **no** form of the command.

shutdown

no shutdown

Syntax Description

This command has no arguments or keywords.

Command Default

Using this command assumes that the interface is already enabled. By default, if this command is not issued, the interface remains enabled.

Command Modes

Controller configuration (config-controller)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Qualified for use in Cisco vManage CLI templates.

Examples

```
Router(config)# controller SHDSL 0/1/0
Router(config-controller)# termination cpe
Router(config-controller)# mode atm
Router(config-controller)# dsl-group 0 pairs 0
Router(config-controller-dsl-group)# shdsl rate auto
...
Router(config-controller-dsl-group)# ignore crc always
Router(config-controller-dsl-group)# shutdown
Router(config-controller-dsl-group)# no shutdown
Router(config-controller-dsl-group)#
```

termination

To configure the termination mode of the controller, use the **termination** command in the controller configuration mode (**controller SHDSL**). You can use the **no** form of the command to configure the default termination mode (cpe), but we recommend configuring the termination mode explicitly.

termination { **co** | **cpe** }

no termination

Syntax Description

co	Set the line termination for the interface as CO (network).
cpe	Termination cpe (customer).

Command Default

The command default termination mode is CPE.

Command Modes

Controller configuration mode (config-controller)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Command qualified for use in Cisco vManage CLI templates.

In the examples, note that SHDSL must be all capital letters.

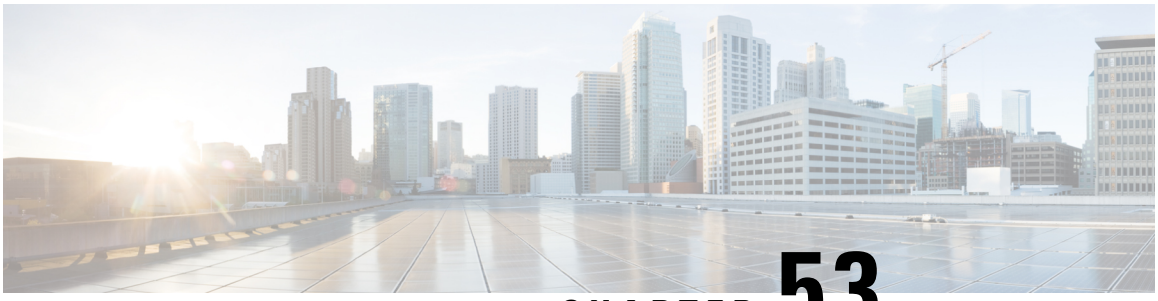
```
Router(config)# controller SHDSL 0/1/0
Router(config-controller)# termination cpe
Router(config-controller)# mode atm
Router(config-controller)# dsl-group 0 pairs 0
Router(config-controller-dsl-group)#
```

```
Router(config)# controller SHDSL 0/1/0
Router(config-controller)# termination cpe
Router(config-controller)# mode atm
Router(config-controller)# dsl-group auto
Router(config-controller-dsl-group)#
```

```
Router(config)# controller SHDSL 0/1/0
Router(config-controller)# termination cpe
Router(config-controller)# mode atm
Router(config-controller)# dsl-group 0 pairs 0-3 m-pair
Router(config-controller-dsl-group)#
```

```
Router(config)# controller SHDSL 0/1/0
Router(config-controller)# termination cpe
Router(config-controller)# mode atm
Router(config-controller)# dsl-group 0 pairs 0
Router(config-controller)# dsl-group 1 pairs 2-3 m-pair
```

```
Router(config)# controller SHDSL 0/1/0
Router(config-controller)# termination cpe
Router(config-controller)# mode efm
Router(config-controller)# dsl-group 0 pairs 0-3 efm-bond
Router(config-controller-dsl-group)#
```



CHAPTER 53

Smart Licensing

- license smart transport, on page 775
- license smart url, on page 776

license smart transport

To choose the type of channel for the smart agent to communicate with Cisco Smart Software Manager, use the **license smart transport** command in global configuration mode.

license smart transport { **smart** | **cslu** | **off** }

no license smart transport

Syntax Description

smart	Connects with Cisco Smart Software Manager (Cisco SSM) using direct connection mode.
cslu	Connects with Cisco SSM using indirect connection mode.
off	Uses offline connection mode to connect with Cisco SSM.

Command Default

cslu is chosen as the connection mode by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco vManage CLI templates.

Example

The following example configures smart transport for communication with Cisco SSM.

```
Device(config)# license smart transport smart
```

The following example configures cslu for all furture communication with Cisco SSM.

```
Device(config)# license smart transport cslu
```

The following example disables all communication betweent he smart agent and Cisco SSM.

```
Device(config)# license smart transport off
```

license smart url

To configure the type of Cisco Smart License Utility URL for the Smart Agent to communicate with Cisco Smart Software Manager (SSM), use the **license smart url** command in global configuration mode.

license smart url { *url* | **cslu** [*transport-url*] }

no license smart url

Syntax Description

cslu	Enables communication with Cisco SSM using the Cisco Smart License Utility.
url	(Optional) The Cisco Smart License Utility URL.
transport-url	(Optional) The Smart Transport URL.

Command Default

When the transport type is configured as smart, a smart URL is created by default. However, when you configure CSLU as the transport type, you need to specify the CSLU URL for successful communication with Cisco SSM.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use for Cisco vManage CLI templates.

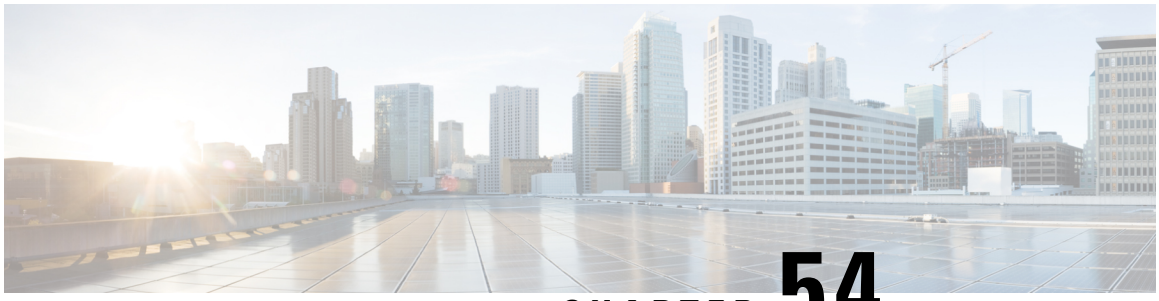
Example

This example configures the transport type as smart and provides a smart URL for the communication between the smart agent and Cisco SSM.

```
Device(config)# license smart url https://smartreceiver-stage.cisco.com/licservice/license
```

This example configure CSLU as the transport type and configures a CSLU URL.

```
Device(config)# license smart url cslu http:10.195.85.83:8182/cslu/v1/pi
```



CHAPTER 54

SNMP Commands

Instructions for SNMP Commands

Note Some configurations and protocols are identified as insecure and is a security risk for Cisco devices. Existing deployments continue to function, but new installations require intentional enablement. For more information on remediation, refer to Resilient Infrastructure: Cisco Catalyst SD-WAN and Routing

- snmp ifmib ifindex persist, on page 778
- snmp mib community-map, on page 778
- snmp-server community, on page 779
- snmp-server contact, on page 781
- snmp-server context, on page 781
- snmp-server enable traps, on page 782
- snmp-server enable traps alarms informational, on page 782
- snmp-server enable traps bgp, on page 783
- snmp-server enable traps config, on page 784
- snmp-server enable traps config-copy, on page 785
- snmp-server enable traps config-ctid, on page 785
- snmp-server enable traps cpu, on page 786
- snmp-server enable traps entity, on page 787
- snmp-server enable traps entity-state, on page 787
- snmp-server enable traps event-manager, on page 788
- snmp-server enable traps flash, on page 788
- snmp-server enable traps memory, on page 789
- snmp-server enable traps ospf cisco-specific errors config-error, on page 790
- snmp-server enable traps ospf errors, on page 790
- snmp-server enable traps ospf lsa, on page 791
- snmp-server enable traps ospf state-change, on page 792
- snmp-server enable traps sdwan, on page 793
- snmp-server enable traps snmp, on page 793
- snmp-server enable traps syslog, on page 794
- snmp-server engineID local, on page 795
- snmp-server engineID remote, on page 795

- snmp-server file-transfer access-group, on page 796
- snmp-server group, on page 797
- snmp-server host, on page 799
- snmp-server location, on page 800
- snmp-server packetsize, on page 800
- snmp-server sparse-tables, on page 801
- snmp-server system-shutdown, on page 802
- snmp-server trap authentication unknown-context, on page 803
- snmp-server trap-source, on page 804
- snmp-server trap timeout, on page 804
- snmp-server user, on page 805
- snmp-server view, on page 807
- snmp trap link-status, on page 808
- tftp-server, on page 809

snmp ifmib ifindex persist

To globally enable ifindex values to persist, 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 router is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

The value remains constant across reboots, for use by SNMP in global configuration mode. For usage guidelines, see the Cisco IOS XE snmp ifmib ifindex persist command.

Examples

The following example shows how to enable ifIndex persistence for all interfaces:

```
Device(config)# snmp ifmib ifindex persist
```

snmp mib community-map

To associate a Simple Network Management Protocol (SNMP) community with an SNMP context, engine ID, or security name, use the **snmp mib community-map** command in global configuration mode. To change an SNMP community mapping to its default mapping, use the **no** form of this command.

snmp mib community-map *community-name* [**engineid** *engine-id*]
no snmp mib community-map *community-name* [**engineid** *engine-id*]

Syntax Description

community-name	String that identifies the SNMP community.
engineid	(Optional) Specifies that an SNMP engine ID is mapped to the SNMP community.
engine-id	String that identifies the SNMP engine ID. Default is the local engine ID

Command Default

No SNMP communities and contexts are associated.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE snmp mib community-map command.

Examples

The following example shows how to specify the SNMP engine ID on the local device, create an SNMP community named community1, and associate the community with with the SNMP engine ID.

```
Device(config)# snmp-server engineID local 876543211234
Device(config)# snmp-server community community1
Device(config)# snmp mib community-map community1 engineid 876543211234
```

snmp-server community

To set up the community access string to permit access to the Simple Network Management Protocol (SNMP), use the **snmp-server community** command in global configuration mode. To remove the specified community string, use the **no**form of this command.

snmp-server community *string* [**view** *view-name*] [**ro** [*access-list-number/name*]]
no snmp-server community *string* [**ro**]

Syntax Description

string	Community string that consists of 1 to 32 alphanumeric characters and functions much like a password, permitting access to SNMP. Blank spaces are not permitted in the community string. **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.
view	(Optional) Specifies a previously defined view. The view defines the objects available to the SNMP community.

view-name	Name of a previously defined view.
ro	(Optional) Specifies read-only access. Authorized management stations can retrieve only MIB objects.
access-list-number/name	(Optional) Integer from 1 to 99 that specifies a standard access list of IP addresses or a string (not to exceed 64 characters) that is the name of a standard access list of IP addresses allowed access to the SNMP agent. Alternatively, an integer from 1300 to 1999 that specifies a list of IP addresses in the expanded range of standard access list numbers that are allowed to use the community string to gain access to the SNMP agent.

Command Default

An SNMP community string permits read-only access to all objects.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE snmp-server community command.

Examples

The following example shows how to set the read only community string to TEST:

```
Device(config)# snmp-server community TEST ro
```

The following example shows how to allow read-only access for all objects to members of the standard named access list ACL1 that specify the TEST community string. No other SNMP managers have access to any objects.

```
Device(config)# snmp-server community TEST ro ACL1
```

The following example shows how to assign the string TEST to SNMP, allow read-only access, and specify that IP access list 4 can use the community string:

```
Device(config)# snmp-server community TEST ro 4
```

The following example shows how to remove the community TEST:

```
Device(config)# no snmp-server community TEST
```

The following example shows how to disable all versions of SNMP:

```
Device(config)# no snmp-server
```

snmp-server contact

To set the system contact (sysContact) string, use the **snmp-server contact** command in global configuration mode. To remove the system contact information, use the **no** form of this command.

snmp-server contact *text*
no snmp-server contact

Syntax Description

text	String that describes the system contact information.

Command Default

No system contact string is set.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Examples

The following is an example of a system contact string:

```
Device(config)#snmp-server contact Bangalore
```

snmp-server context

To create an SNMP context, use the **snmp-server context** command in global configuration mode. To delete an SNMP context, use the **no** form of this command.

snmp-server context *context-name*
no snmp-server context *context-name*

Syntax Description

context-name	Name of the SNMP context being created.

Command Default

No SNMP contexts are configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE snmp-server context command.

Examples

The following example shows how to create an SNMP context named contextA and associate it with a virtual private network (VPN) routing and forwarding (VRF) instance named CustomerA:

```
Device(config)# snmp-server context contextA
Device(config)# ip vrf CustomerA
Device(config-vrf)# rd 100:120
Device(config-vrf)# context contextA
```

snmp-server enable traps

To enable all Simple Network Management Protocol (SNMP) notification types that are available on your system, use the **snmp-server enable traps**command in global configuration mode. To disable all available SNMP notifications, use the **no**form of this command.

snmp-server enable traps
no snmp-server enable traps

Syntax Description

This command has no keywords or arguments.

Command Default

No notifications controlled by this command are sent.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE snmp-server enable traps command.

Examples

The following example shows how to enable all notification types available on your device:

```
Device(config)# snmp-server enable traps
```

snmp-server enable traps alarms informational

To enable alarm SNMP notifications, use the **snmp-server enable traps alarms** command in global configuration mode. To disable SNMP notifications, use the **no** form of this command.

snmp-server enable traps alarms *severity*
no snmp-server enable traps alarms *severity*

Syntax Description

alarms	Enables alarm filtering to limit the number of syslog messages generated. Alarms are generated for the severity configured as well as for the higher severity values.

severity	The severity argument is an integer or string value that identifies the severity of an alarm. Integer values are from 1 to 4. String values are critical, major, minor, and informational. The default is 4 (informational). Severity levels are defined as follows: • 1--Critical: The condition affects service. • 2--Major: Immediate action is needed. • 3--Minor: Minor warning conditions. • 4--Informational: No action is required. This is the default.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE snmp-server enable traps command.

Examples

```
Device(config)# snmp-server enable traps alarms informational
```

snmp-server enable traps bgp

To enable Border Gateway Protocol (BGP) support for SNMP operations on a router, use the **snmp-server enable traps bgp** command in global configuration mode. To disable BGP support for SNMP operations, use the **no** form of this command.

snmp-server enable traps bgp [**cbgp2**] [**state-changes** [**all**] [**backward-trans**] [**limited**] | **threshold prefix**]
no snmp-server enable traps bgp [**cbgp2**] [**state-changes** [**all**] [**backward-trans**] [**limited**] | **threshold prefix**]

Syntax Description

cbgp2	(Optional) Enables generation of the CISCO-BGP-MIBv8.1 traps.
state-changes	(Optional) Enables traps for finite state machine (FSM) state changes.
all	(Optional) Enables Cisco specific traps for all FSM state changes.
backward-trans	(Optional) Enables Cisco specific traps for backward transition events.
limited	(Optional) Enables traps for standard backward transition and established events.
threshold prefix	(Optional) Enables Cisco-specific trap for prefix threshold events.

Command Default

By default, SNMP notifications are disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

If you have Cisco Catalyst SD-WAN Manager Release 20.15.3 and Cisco IOS XE Catalyst SD-WAN Release 17.12.2a, then update the cli template with the **snmp-server enable traps bgp-dep** command.

For usage guidelines, see the Cisco IOS XE snmp-server enable traps bgp command.

Examples

The following example enables the router to send BGP state change informs to the host at the address myhost.cisco.com using the community string defined as public:

```
Device(config)# snmp-server enable traps bgp
Device(config)# snmp-server host myhost.cisco.com informs version 2c public
```

The following example enables generation of the CISCO-BGP-MIBv8.1 traps:

```
Device(config)# snmp-server enable traps bgp cbgp2
```

snmp-server enable traps config

To enable SNMP trap notifications for configuration activity, use the **snmp-server enable traps config** command in global configuration mode. To disable SNMP trap notifications, use the **no** form of this command.

snmp-server enable traps config
no snmp-server enable traps config

Syntax Description

config	Controls configuration notifications, as defined in the CISCO-CONFIG-MAN-MIB (enterprise 1.3.6.1.4.1.9.9.43.2). The notification type is (1) ciscoConfigManEvent.

Command Default

No notifications controlled by this command are sent.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE snmp-server enable traps command.

Example

```
Device(config)# snmp-server enable traps config
```

snmp-server enable traps config-copy

To send config-copy notifications to Cisco SD-WAN Manager or to the Simple Network Management Protocol (SNMP) manager, indicating successful completion of the config-copy operation to or from an SNMP agent, use the **snmp-server enable traps config-copy** command in global configuration mode. To disable sending notifications, use the **no** form of this command.

snmp-server enable traps config-copy
no snmp-server enable traps config-copy

Syntax Description

config-copy	Facilitates the task of copying SNMP agent configuration files to the startup configuration or to the local Cisco IOS file system, and vice versa.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

The Config-Copy MIB facilitates the copying of SNMP agent configuration files to the startup configuration or the local Cisco IOS file system, and vice versa. The config-copy notifications are sent to Cisco SD-WAN Manager or the SNMP manager to indicate the successful completion of the config-copy operation to or from the SNMP agent.

Examples

The following example shows how to configure config-copy traps to simulate the verification of config-copy traps:

```
Device(config)# snmp-server enable traps config-copy
```

snmp-server enable traps config-ctid

To enable configuration change tracking identifier (CTID) notifications, use the **snmp-server enable traps config-ctid** command in global configuration mode. To disable CTID notifications, use the **no** form of this command.

snmp-server enable traps config-ctid
no snmp-server enable traps config-ctid

Syntax Description

config-ctid	Specifies the configuration change tracking identifier.

Command Default

This command is disabled by default. If this command isn't run, the management system has to query the device for the current running-config file and then compare the results with the last-known configuration to determine if a change has been made.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

This configuration infrastructure command assigns a version number that is updated every time the running-config file is changed. This version number is called the configuration change tracking identifier (CTID). This identifier assigns a version number to each saved version of the running-config file. The CTID can be used to compare configuration files to track configuration changes and take appropriate actions, for example, a configuration rollback. Config Logger can also use the CTID to determine if there have been any changes to the running-config file.

CTID makes the management system more efficient by presenting information that indicates a change has been made to the running-config file. Without CTID, the management system has to query the device for the current running-config file and then compare the results with the last-known configuration to determine if a change has been made.

Examples

The following example shows how to enable configuration change tracking identifier (CTID) notifications:

```
Device(config)# snmp-server enable traps config-ctid
```

snmp-server enable traps cpu

To enable a device to send CPU thresholding violation notifications, use the **snmp-server enable traps cpu** command in global configuration mode. To stop a device from sending CPU threshold notifications, use the **no** form of this command.

snmp-server enable traps cpu threshold
no snmp-server enable traps cpu

Syntax Description

threshold	Enables notifications of CPU threshold violations.

Command Default

SNMP notifications are disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE snmp-server enable traps cpu command.

Examples

The following example shows how to enable a device to send CPU threshold-related information to the host at the address myhost.cisco.com using the community string defined as public:

```
Device(config)# snmp-server enable traps cpu threshold
Device(config)# snmp-server host myhost.cisco.com informs version 2c public cpu
```

snmp-server enable traps entity

To send entity MIB notifications to a host, use the **snmp-server enable traps entity** command in global configuration mode. To disable SNMP notifications, use the **no** form of this command.

snmp-server enable traps entity
no snmp-server enable traps entity

Syntax Description

entity	Controls Entity MIB modify notifications. This notification type is defined in the ENTITY-MIB (enterprise 1.3.6.1.2.1.47.2) as (1) entConfigChange.

Command Default

By default, the command is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Examples

```
Device(config)# snmp-server enable traps entity
```

snmp-server enable traps entity-state

To send information about the state of physical components such as disk, memory, and CPU utilization, use the **snmp-server enable traps entity-state** command in global configuration mode. To disable sending information about physical components, use the **no** form of this command.

snmp-server enable traps entity-state
no snmp-server enable traps entity-state

Syntax Description

This command has no keywords or arguments.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Examples

```
Device(config)# snmp-server enable traps entity-state
```

snmp-server enable traps event-manager

To permit Simple Network Management Protocol (SNMP) traps to be sent from the Cisco IOS XE Catalyst SD-WAN devices to the SNMP server, enable the **snmp-server enable traps event-manager** command in global configuration mode. Other relevant **snmp-server** commands must also be configured. For details see the **action snmp-trap** command page. To stop sending SNMP traps to the server, use the **no** form of this command.

snmp-server enable traps event-manager
no snmp-server enable traps event-manager

Syntax Description

event-manager	Enables SNMP-embedded event manager traps.

Command Default

No Embedded Event Manager (EEM) traps are registered.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Examples

The following example shows how to enable SNMP-embedded event manager traps:

```
Device(config)# snmp-server enable traps event-manager
```

snmp-server enable traps flash

To enable flash device insertion and removal Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps flash** command in global configuration mode. To disable flash device SNMP notifications, use the **no** form of this command.

snmp-server enable traps flash [**insertion** | **lowspace** | **removal**]
no snmp-server enable traps flash

Syntax Description

insertion	(Optional) Controls flash card insertion notifications.
low space	(Optional) Controls flash card low-space notifications.
removal	(Optional) Controls flash card removal notifications.

Command Default

SNMP notifications are disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE snmp-server enable traps flash command.

Examples

The following example shows how to enable a device to send information relating to flash card insertion, low space, and removal to the host at the address myhost.cisco.com using the community string defined as public:

```
Device(config)# snmp-server enable traps flash insertion lowspace removal
Device(config)# snmp-server host myhost.cisco.com informs version 2c public flash
```

snmp-server enable traps memory

To enable a device to send Simple Network Management Protocol (SNMP) notifications when memory pool buffer usage reaches a new peak, use the **snmp-server enable traps memory** command in global configuration mode. To stop notifications from being generated, use the **no** form of this command.

snmp-server enable traps memory [**bufferpeak**]
no snmp-server enable traps memory [**bufferpeak**]

Syntax Description

bufferpeak	(Optional) Specifies memory buffer peak notifications.

Command Default

SNMP notifications in the MEMPOOL-MIB are not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE snmp-server enable traps memory command.

Examples

The following example shows how to configure memory traps to enable all the available memory-related SNMP notifications and configured to be sent as information to the host myhost.cisco.com using the community string public:

```
Device(config)# snmp-server enable traps memory
Device(config)# snmp-server host myhost.cisco.com informs version 3 public memory
```

snmp-server enable traps ospf cisco-specific errors config-error

To enable SNMP notifications for Open Shortest Path First (OSPF) nonvirtual interface mismatch errors, use the **snmp-server enable traps ospf cisco-specific errors config-error** command in global configuration mode. To disable OSPF nonvirtual interface mismatch error SNMP notifications, use the **no** form of this command.

snmp-server enable traps ospf cisco-specific errors config-error
no snmp-server enable traps ospf cisco-specific errors config-error

Syntax Description

This command has no keywords or arguments.

Command Default

This command is disabled by default; therefore, SNMP notifications for OSPF nonvirtual interface mismatch errors are not created.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE snmp-server enable traps ospf cisco-specific errors command.

Examples

The following example enables the router to send nonvirtual interface mismatch error notifications to the host at the address myhost.cisco.com using the community string defined as public:

```
Device(config)# snmp-server enable traps ospf cisco-specific errors config-error
Device(config)# snmp-server host myhost.cisco.com informs version 2c public
```

snmp-server enable traps ospf errors

To enable SNMP notifications for Open Shortest Path First (OSPF) errors, use the **snmp-server enable traps ospf errors** command in global configuration mode. To disable SNMP notifications for OSPF errors, use the **no** form of this command.

snmp-server enable traps ospf errors [**authentication-failure**] [**bad-packet**] [**config-error**] [**virt-authentication-failure**] [**virt-bad-packet**] [**virt-config-error**]
no snmp-server enable traps ospf errors [**authentication-failure**] [**bad-packet**] [**config-error**] [**virt-authentication-failure**] [**virt-bad-packet**] [**virt-config-error**]

Syntax Description

authentication-failure	(Optional) Enables only the ospfIfFailure trap. Allows SNMP notifications to be sent when a packet has been received on a nonvirtual interface from a neighbor router whose authentication key or authentication type conflicts with the authentication key or authentication type of this router.

bad-packet	(Optional) Enables only the ospfIfRxBadPacket trap. Allows SNMP notifications to be sent when an OSPF packet that has not been parsed has been received on a nonvirtual interface.
config-error	(Optional) Enables only the ospfIfConfigError trap. Sends SNMP notifications when a packet has been received in a nonvirtual interface from a neighbor router whose configuration parameters conflict with the configuration parameters of this router.
virt-authentication-failure	(Optional) Enables only the ospfVirtIfFailure trap. Allows SNMP notifications to be sent when a packet has been received on a virtual interface from a neighbor router whose authentication key or authentication type conflicts with the authentication key or authentication type of this router.
virt-bad-packet	(Optional) Enables only the ospfVirtIfRxBadPacket trap. Allows SNMP notifications to be sent when an OSPF packet that has not been parsed has been received on a virtual interface.
virt-config-error	(Optional) Enables only the ospfVirtIfConfigError trap. Sends SNMP notifications when a packet has been received in a virtual interface from a neighbor router whose configuration parameters conflict with the configuration parameters of this router.

Command Default

SNMP notifications for OSPF errors are disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE snmp-server enable traps ospf errors command.

Examples

The following example enables the router to send all OSPF error notifications:

```
Device(config)# snmp-server enable traps ospf errors
```

snmp-server enable traps ospf lsa

To enable SNMP notifications for Open Shortest Path First (OSPF) link-state advertisements (LSAs), use the **snmp-server enable traps ospf lsa** command in global configuration mode. To disable SNMP notifications for OSPF LSAs, use the **no** form of this command.

snmp-server enable traps ospf lsa [**lsa-maxage**] [**lsa-originate**]
no snmp-server enable traps ospf lsa [**lsa-maxage**] [**lsa-originate**]

Syntax Description

lsa-maxage	(Optional) Enables only the ospfMaxAgeLsa trap. Allows SNMP notifications to be sent when an LSA in the OSPF link-state database of the router has reached the maximum age.

lsa-originate	(Optional) Enables only the ospfOriginateLsa trap. Enables SNMP notifications when a new LSA has been originated by the router as a result of a topology change.

Command Default SNMP notifications for OSPF LSAs are disabled.

Command Modes Global configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines For usage guidelines, see the Cisco IOS XE snmp-server enable traps ospf lsa command.

Examples

The following example enables the router to send SNMP notifications when new LSAs are originated by the router as a result of a topology change:

```
Device(config)# snmp-server enable traps ospf lsa lsa-originate
```

snmp-server enable traps ospf state-change

To enable SNMP notifications for Open Shortest Path First (OSPF) transition state changes, use the **snmp-server enable traps ospf state-change** command in global configuration mode. To disable SNMP notifications for OSPF transition state changes, use the **no** form of this command.

snmp-server enable traps ospf state-change
no snmp-server enable traps ospf state-change

Syntax Description This command has no arguments or keywords.

Command Default SNMP notifications for OSPF transition state changes are disabled.

Command Modes Global configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines To enable all traps for transition state changes, enter the **snmp-server enable traps ospf state-change** command.

Examples

The following example enables the router to send SNMP notifications for transition state changes:

```
Device(config)# snmp-server enable traps ospf state-change
```

snmp-server enable traps sdwan

To enable all ciscoSdwan traps, use **snmp-server enable traps sdwan** command. To disable traps, use the **no** form of this command.

snmp-server enable traps sdwan
no snmp-server enable traps sdwan

Syntax Description

This command has no keywords or arguments.

Command Default

ciscoSdwan traps are disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Examples

```
Device(config)# snmp-server enable traps sdwan
```

snmp-server enable traps snmp

To enable the RFC 1157 Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps snmp**command in global configuration mode. To disable RFC 1157 SNMP notifications, use the **no**form of this command.

snmp-server enable traps snmp [**authentication**] [**linkup**] [**linkdown**] [**coldstart**] [**warmstart**]
no snmp-server enable traps snmp [**authentication**] [**linkup**] [**linkdown**] [**coldstart**] [**warmstart**]

Syntax Description

authentication	(Optional) Controls the sending of SNMP authentication failure notifications.
linkup	(Optional) Controls the sending of SNMP linkUp notifications.
linkdown	(Optional) Controls the sending of SNMP linkDown notifications.
coldstart	(Optional) Controls the sending of SNMP coldStart notifications.
warmstart	(Optional) Controls the sending of SNMP warmStart notifications.

Command Default

SNMP notifications are disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Command qualified for use in Cisco vManage CLI templates.

For usage guidelines, see the Cisco IOS XE snmp-server enable traps snmp command.

Examples

The following example shows how to enable various SNMP trap types.

```
Device(config)# snmp-server enable traps snmp authentication

Device(config)# snmp-server enable traps snmp coldstart

Device(config)# snmp-server enable traps snmp linkdown

Device(config)# snmp-server enable traps snmp linkup

Device(config)# snmp-server enable traps snmp warmstart
```

snmp-server enable traps syslog

To enable sending of system logging message Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps syslog** command in global configuration mode. To disable sending SNMP notifications, use the **no** form of this command.

snmp-server enable traps syslog
no snmp-server enable traps syslog

Syntax Description

This command has no arguments or keywords.

Command Default

SNMP notifications are disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE snmp-server enable traps syslog command.

Examples

The following example shows how to enable the device to send system logging messages at severity levels 0 (emergencies) through 2 (critical) to the host at the address myhost.cisco.com using the community string defined as public:

```
Device(config)# snmp-server enable traps syslog
Device(config)# logging history 2
Device(config)# snmp-server host myhost.cisco.com traps version 2c public
```

snmp-server engineID local

To specify the Simple Network Management Protocol (SNMP) engine ID on the local device, use the **snmp-server engineID local** command in global configuration mode. To remove the configured engine ID, use the **no** form of this command.

snmp-server engineID local *engineid-string*
no snmp-server engineID local

Syntax Description

engineid-string	String of a minimum of 10 characters and a maximum of 64 characters that identifies the engine ID.

Command Default

An SNMP engine ID is generated automatically but is not displayed or stored in the running configuration. You can display the default or configured engine ID by using the **show snmp engineID** command.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE snmp-server engineID local command.

Examples

The following example specifies the local SNMP engine ID:

```
Device(config)# snmp-server engineID local
```

snmp-server engineID remote

To specify the Simple Network Management Protocol (SNMP) engine ID of a remote SNMP device, use the **snmp-server engineID remote** command in global configuration mode. To remove a specified SNMP engine ID from the configuration, use the **no** form of this command.

snmp-server engineID remote *ipv4-address* [**udp-port** *udp-port-number*] [**vrf** *vrf-name*] [*engineid-string*]
no snmp-server engineID remote *ipv4-address* [**udp-port** *udp-port-number*] [**vrf** *vrf-name*] [*engineid-string*]

Syntax Description

ipv4-address	IPv4 address of the device that contains the remote copy of SNMP.
udp-port	(Optional) Specifies a User Datagram Protocol (UDP) port of the host to use.
udp-port-number	(Optional) Socket number on the remote device that contains the remote copy of SNMP. The default is 161.

vrf	(Optional) Specifies an instance of a routing table.
vrf-name	(Optional) Name of the Virtual Private Network (VPN) routing and forwarding (VRF) table to use for storing data.
engineid-string	String of a maximum of 64 characters and minimum of 10 characters that identifies the engine ID.

Command Default

The default is UDP port 161.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE snmp-server engineID remote command.

Example

The following example specifies the SNMP engine ID and configures the VRF name BLR for SNMP communications with the remote device at 172.16.20.3:

```
Device(config)# snmp-server engineID remote 172.16.20.3 vrf BLR
80000009030000B064EFE100
```

The following example specifies the SNMP engine ID and UDP port for SNMP communications with the remote device at 10.1.1.1:

```
Device(config)# snmp-server engineID remote 10.1.1.1 udp-port 10 abcdef1234
```

snmp-server file-transfer access-group

To associate an access list to the transfer protocols TFTP, FTP, Remote Copy Protocol (RCP), Secure Copy Protocol (SCP), and Secured File Transfer Protocol (SFTP), use the **snmp-server file-transfer access-group** command in global configuration mode. To disassociate an access list, use **no** form of this command.

snmp-server file-transfer access-group { *acl-number* | *acl-name* }
no snmp-server file-transfer access-group

Syntax Description

acl-number	Integer from 1 to 99 that specifies a standard ACL.
acl-name	String that specifies a standard ACL.

Command Default

If a protocol is not specified, all protocols are associated with the access list.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Command qualified for use in Cisco vManage CLI templates.

For usage guidelines, see the Cisco IOS XE snmp-server file-transfer access-group command.

Examples

The following example shows that configuration transfers that are initiated through SNMP are associated with access list 10 for all the protocols.

```
Device(config)# snmp-server file-transfer access-group 10
```

snmp-server group

To configure a new Simple Network Management Protocol (SNMP) group, use the **snmp-server group** command in global configuration mode. To remove a specified SNMP group, use the **no** form of this command.

snmp-server group *group-name* **v3** { **auth** | **noauth** | **priv** } [**read** *read-view*] [**write** *write-view*] [**notify** *notify-view*] [**access** [*acl-number* | *acl-name*] [**ipv6** *named-access-list*]]
no snmp-server group *group-name* **v3** { **auth** | **noauth** | **priv** } [**read** *read-view*] [**write** *write-view*] [**notify** *notify-view*] [**access** [*acl-number* | *acl-name*] [**ipv6** *named-access-list*]]

Syntax Description

group-name	Name of the group.
v3	Specifies that the group is using the SNMPv3 security model. SMNPv3 is the most secure of the supported security models. It allows you to explicitly configure authentication characteristics.
auth	Specifies authentication of a packet without encrypting it.
noauth	Specifies no authentication of a packet.
priv	Specifies authentication of a packet with encryption.
read	Specifies a read view for the SNMP group. This view enables you to view only the contents of the agent.
read-view	String of a maximum of 64 characters that is the name of the view. The default is that the read-view is assumed to be every object belonging to the Internet object identifier (OID) space (1.3.6.1), unless the **read** option is used to override this state.
write	(Optional) Specifies a write view for the SNMP group. This view enables you to enter data and configure the contents of the agent.
write-view	(Optional) String of a maximum of 64 characters that is the name of the view. The default is that nothing is defined for the write view (that is, the null OID). You must configure write access.

notify	(Optional) Specifies a notify view for the SNMP group. This view enables you to specify a notify, inform, or trap.
notify-view	(Optional) String of a maximum of 64 characters that is the name of the view. By default, nothing is defined for the notify view (that is, the null OID) until the **snmp-server host** command is configured. If a view is specified in the **snmp-server group** command, any notifications in that view that are generated will be sent to all users associated with the group (provided a SNMP server host configuration exists for the user). Cisco recommends that you let the software autogenerate the notify view. See the "Configuring Notify Views" section in this document.
access	(Optional) Specifies a standard access control list (ACL) to associate with the group.
acl-number	The *acl-number*argument is an integer from 1 to 99 that identifies a previously configured standard access list.
acl-name	The *acl-name* argument is a string of a maximum of 64 characters that is the name of a previously configured standard access list.
ipv6	(Optional) Specifies an IPv6 named access list. If both IPv6 and IPv4 access lists are indicated, the IPv6 named access list must appear first in the list.
named-access-list	(Optional) Name of the IPv6 access list.

Command Default

No SNMP server groups are configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Additional parameters qualified: **priv** (specifies authenticating a packet with encryption), **access** (allows you to specify an ACL to associate with a group), and **ipv6** (allows you to specify an IPv6 named access list).

Usage Guidelines

For usage guidelines, see the Cisco IOS XE snmp-server group command.

Examples

Create an SNMP Group

The following example shows how to create the SNMP server group "public", allowing read-only access for all objects to members of the standard named access list "view-public":

```
Device(config)# snmp-server group public v3 noauth read view-public
```

```
Device(config)# snmp-server group public v3 priv read view-public access 5
```

snmp-server host

To specify the recipient of a Simple Network Management Protocol (SNMP) notification operation, use the **snmp-server host** command in global configuration mode. To remove the specified host from the configuration, use the **no** form of this command.

snmp-server host *ip-address* { **vrf** *vrf-name* **version** [**2c** *string* **udp-port** *port*] | **version 3 noauth** *string* [**udp-port** *port*] }
no snmp-server host *ip-address* { **vrf** *vrf-name* **version** [**2c** *string* **udp-port** *port*] | **version 3 noauth** *string* [**udp-port** *port*] }

Syntax Description

ip-address	IPv4 address or IPv6 address of the SNMP notification host.
vrf	Specifies that a VPN routing and forwarding (VRF) instance should be used to send SNMP notifications.
vrf-name	VPN VRF instance used to send SNMP notifications.
version	Specifies the version of the SNMP that is used to send the traps or informs. The default is 1. One of the following three optional security level keywords can follow the **3** keyword:
2c	Specifies SNMPv2C as the SNMP version.
3	Specifies SNMPv3 as the SNMP version.
noauth	Specifies that the noAuthNoPriv security level applies to this host. This is the default security level for SNMPv3.
string	Password-like community string sent with the notification operation. **Note** You can set this string using the **snmp-server host** command by itself, but we recommend that you define the string using the **snmp-server community** command prior to using the **snmp-server host** command. **Note** The "at" sign (@) is used for delimiting the context information.
udp-port	Specifies that SNMP traps or informs are to be sent to an network management system (NMS) host.
port	User Datagram Protocol (UDP) port number of the NMS host. The default is 162.

Command Default

This command behavior is disabled by default. A recipient is not specified to receive notifications.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE snmp-server host command.

Examples

```
Device(config)# snmp-server host 10.100.51.1 vrf 1 version 2c TEST udp-port 7081
Device(config)# snmp-server host 10.1.15.15 version 3 noauth TEST5 udp-port 161
```

snmp-server location

To set the system location string, use the **snmp-server location** command in global configuration mode. To remove the location string, use the **no** form of this command.

snmp-server location *text*
no snmp-server location

Syntax Description

text	String that describes the system location information.

Command Default

No system location string is set.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Examples

The following example shows how to set a system location string:

```
Device(config)# snmp-server location Bengaluru
```

snmp-server packetsize

To establish control over the largest Simple Network Management Protocol (SNMP) packet size permitted when the SNMP server is receiving a request or generating a reply, use the **snmp-server packetsize** command in global configuration mode. To restore the default value, use the **no** form of this command.

snmp-server packetsize *byte-count*
no snmp-server packetsize

Syntax Description

byte-count	Integer from 484 to 17892. The default is 1500.

Command Default

Packet size is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Command qualified for use in Cisco vManage CLI templates.

Examples

The following example establishes a packet filtering of a maximum size of 1024 bytes:

```
Device(config)# snmp-server packetsize 1024
```

snmp-server sparse-tables

To populate all the Simple Network Management Protocol (SNMP) tables when an object ID is applicable, use the **snmp-server sparse-tables** command in global configuration mode. To populate all the SNMP tables even if an object ID is not applicable in a specific case, use the **no** form of this command.

snmp-server sparse-tables [**community** *text* | **contact** *text* | **context** *context-name* | **enable** | **engineID** *engineID-string* | **file-transfer access-group** | **group** *group-name* | **host** *host-name* | **ifindex persist** | **ip** | **location** *text* | **packetsize** *byte-count* | **source-interface** *byte-count* | **trap** | **trap-source** *interface* | **view** *view-name*]
no snmp-server sparse-tables [*notification-types*]

Syntax Description

community *text*	(Optional) Community string that consists of 1 to 32 alphanumeric characters and functions, much like a password permitting access to SNMP. Blank spaces aren't permitted in the community string. **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.
contact *text*	(Optional) Specifies a string that describes the system contact information.
context *context-name*	(Optional) Specifies the name of the SNMP context being created.
enable	(Optional) Enables traps or logging types of SNMP notifications that are available in your system.
engineID *engineID-string*	(Optional) Specifies the SNMP engine ID in the local or remote devices. This can be a string having a maximum of 24 characters.

file-transfer access-group	(Optional) Associates an access list to the transfer protocols TFTP, FTP, Remote Copy Protocol (RCP), Secure Copy Protocol (SCP), and Secured File Transfer Protocol (SFTP).
group *group-name*	(Optional) Configures a new SNMP group. Supports SNMPv3 security model group.
host *host-name*	(Optional) Specifies the recipient of an SNMP notification operation. The SNMP notification host is typically a network management station (NMS) or SNMP manager. This IPv4 or IPv6 SNMP notification host is the recipient of the SNMP traps or information.
ifindex persist	(Optional) Enables ifindex values to persist, which remains constant across reboots, for use by SNMP.
ip	(Optional) Enables sending of local IP SNMP notifications.
location *text*	(Optional) Specifies a string that describes the system location information.
packetsize *byte-count*	(Optional) Specifies the packet size that is permitted when the SNMP server is receiving a request or generating a reply. Byte count is an integer from 484 to 8192. The default is 1500.
source-interface *byte-count*	(Optional) Specifies the interface from which an SNMP trap originates.
trap	(Optional) Enables trap type of notification.
trap-source *interface*	(Optional) Specifies the interface (and hence the corresponding IP address) from which an SNMP trap should originate.
view *view-name*	(Optional) Creates or updates a view entry. View name is used to reference the record. Label for the view record that you're updating or creating.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Examples

The following example shows how to set the read/write community string to newstring:

```
Device(config)# snmp-server sparse-tables community newstring rw
```

snmp-server system-shutdown

To enable the SNMP message reload feature, use the **snmp-server system-shutdown** command in global configuration mode. To prevent an SNMP system-shutdown request (from an SNMP manager) from resetting the Cisco agent, use the **no** form of this command.

snmp-server system-shutdown

no snmp-server system-shutdown

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	This command was introduced.

Usage Guidelines For usage guidelines, see the Cisco IOS XE snmp-server system-shutdown command.

Examples The following example shows how to enable the SNMP message reload feature:

```
Device(config)# snmp-server system-shutdown
```

snmp-server trap authentication unknown-context

To enable the SNMP authorization failure (authFail) traps during an unknown context error, use the **snmp-server trap authentication unknown-context** command in global configuration mode. To disable the authFail traps, use the **no** form of this command.

snmp-server trap authentication unknown-context
no snmp-server trap authentication unknown-context

Syntax Description This command has no arguments or keywords.

Command Default By default, authfail is enabled.

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Examples The following example shows how to enable the authorization failure traps during an unknown context error:

```
Device(config)# snmp-server trap authentication unknown-context
```

The following example shows how to disable the authorization failure traps during an unknown context error:

```
Device(config)# no snmp-server trap authentication unknown-context
```

snmp-server trap-source

To specify the interface (and hence the corresponding IP address) from which a Simple Network Management Protocol (SNMP) trap should originate, use the **snmp-server trap-source** command in global configuration mode. To remove the source designation, use the **no** form of the command.

snmp-server trap-source Loopback *number*
no snmp-server trap-source

Syntax Description

number	Specifies the interface number. The range is <0..4294967295>

Command Default

No interface is specified.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE snmp-server trap-source command.

Examples

Please verify the following example and provide a description for the same

```
Device(config)# snmp-server trap-source Loopback 10
```

snmp-server trap timeout

To define an interval of time between retransmissions of trap messages on a retransmission queue, use the **snmp-server trap timeout** command in global configuration mode.

To remove the interval defined, use the **no** form of this command.

snmp-server trap timeout *seconds*
no snmp-server trap timeout

Syntax Description

seconds	Integer from 1 to 1000 that sets the interval, in seconds, for resending messages. The default is 30.

Command Default

This command is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE snmp-server trap timeout command.

Examples

The following example shows how to set an interval of 100 seconds between retransmissions of traps:

```
Device(config)# snmp-server trap timeout 100
```

snmp-server user

To configure a new user to a SNMP group, use the **snmp-server user** command in global configuration mode. To remove a user from an SNMP group, use the **no** form of this command.

snmp-server user *username group-name* [**remote** *host* [**udp-port** *port*] [**vrf** *vrf-name*]] { **v1** | **v2c** | **v3** [**encrypted**] [**auth** { **md5** | **sha** } *auth-password*] } [**access** [**ipv6** *nacl*] [**priv** { **des** | **3des** | **aes** { **128** | **192** | **256** } } *privpassword*] { *acl-number acl-name* }]
no snmp-server user *username group-name* [**remote** *host* [**udp-port** *port*] [**vrf** *vrf-name*]] { **v1** | **v2c** | **v3** [**encrypted**] [**auth** { **md5** | **sha** } *auth-password*] } [**access** [**ipv6** *nacl*] [**priv** { **des** | **3des** | **aes** { **128** | **192** | **256** } } *privpassword*] { *acl-number acl-name* }]

Syntax Description

username	Name of the user on the host that connects to the agent.
group-name	Name of the group to which the user belongs.
remote	(Optional) Specifies a remote SNMP entity to which the user belongs, and the hostname or IPv6 address or IPv4 IP address of that entity. If both an IPv6 address and IPv4 IP address are being specified, the IPv6 host must be listed first.
host	(Optional) Name or IP address of the remote SNMP host.
udp-port	(Optional) Specifies the User Datagram Protocol (UDP) port number of the remote host.
port	(Optional) Integer value that identifies the UDP port. The default is 162.
vrf	(Optional) Specifies an instance of a routing table.
vrf-name	(Optional) Name of the Virtual Private Network (VPN) routing and forwarding (VRF) table to use for storing data.
v1	Specifies that SNMPv1 should be used.
v2c	Specifies that SNMPv2c should be used.

v3	Specifies that the SNMPv3 security model should be used. Allows the use of the **encrypted** keyword or **auth** keyword or both.
encrypted	(Optional) Specifies whether the password appears in encrypted format.
auth	(Optional) Specifies which authentication level should be used.
md5	(Optional) Specifies the HMAC-MD5-96 authentication level.
sha	(Optional) Specifies the HMAC-SHA-96 authentication level.
auth-password	(Optional) String (not to exceed 64 characters) that enables the agent to receive packets from the host.
access	(Optional) Specifies an Access Control List (ACL) to be associated with this SNMP user.
ipv6	(Optional) Specifies an IPv6 named access list to be associated with this SNMP user.
nacl	(Optional) Name of the ACL. IPv4, IPv6, or both IPv4 and IPv6 access lists may be specified. If both are specified, the IPv6 named access list must appear first in the statement.
priv	(Optional) Specifies the use of the User-based Security Model (USM) for SNMP version 3 for SNMP message level security.
des	(Optional) Specifies the use of the 56-bit Digital Encryption Standard (DES) algorithm for encryption.
3des	(Optional) Specifies the use of the 168-bit 3DES algorithm for encryption.
aes	(Optional) Specifies the use of the Advanced Encryption Standard (AES) algorithm for encryption.
128	(Optional) Specifies the use of a 128-bit AES algorithm for encryption.
192	(Optional) Specifies the use of a 192-bit AES algorithm for encryption.
256	(Optional) Specifies the use of a 256-bit AES algorithm for encryption.
privpassword	(Optional) String (not to exceed 64 characters) that specifies the privacy user password.
acl-number	(Optional) Integer in the range from 1 to 99 that specifies a standard access list of IP addresses.
acl-name	(Optional) String (not to exceed 64 characters) that is the name of a standard access list of IP addresses.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE snmp-server user command.

Examples

The following example configures a new user with an authentication and an authentication password and a privacy and privacy password, to receive traps at the priv security level when the SNMPv3 security model is enabled:

```
Device(config)# snmp-server user v3user AuthPriv groupAuthPriv v3 auth sha <PASSWORD> priv
 aes 128 <PASSWORD>
```

The following example configures a new user with an authentication and an authentication password, to receive traps at the authNoPriv security level when the SNMPv3 security model is enabled:

```
Device(config)# snmp-server user v3user AuthNoPriv groupAuthNoPriv v3 auth sha <PASSWORD>
```

The following example configures a new user without authentication or privacy credentials, to receive traps at the noAuthNoPriv security level when the SNMPv3 security model is enabled:

```
Device(config)# snmp-server user v3user NoAuthNoPriv groupNoAuthNoPriv v3
```

Note The **show running-config** command does not display any of the active SNMP users created in authPriv or authNoPriv mode, though it does display the users created in noAuthNoPriv mode. To display any active SNMPv3 users created in authPriv, authNoPrv, or noAuthNoPriv mode, use the **show snmp user** command.

snmp-server view

To create or update a view entry, use the **snmp-server view** command in global configuration mode. To remove the specified Simple Network Management Protocol (SNMP) server view entry, use the **no**form of this command.

snmp-server view *view-name oid-tree* **included**
no snmp-server view *view-name*

Syntax Description

view-name	Label for the view record that you are updating or creating. The name is used to reference the record.
oid-tree	Object identifier of the ASN.1 subtree to be included or excluded from the view. To identify the subtree, specify a text string consisting of numbers, such as 1.3.6.2.4, or a word, such as system. Replace a single subidentifier with the asterisk (*) wildcard to specify a subtree family; for example 1.3.*.4.
included	Configures the OID (and subtree OIDs) specified in *oid-tree* argument to be included in the SNMP view.

Command Default

No view entry exists.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE snmp-server view command.

Examples

In the following example, A view name TEST is created, which includes the MIB tree under 1.3.1 OID. Therefore, this view can be used to access the objects under the MIB tree 1.3.1 only.

```
Device(config)# snmp-server view TEST 1.3.1 included
```

snmp trap link-status

To enable Simple Network Management Protocol (SNMP) link trap generation when the interface state changes, use the **snmp trap link-status** command in interface configuration mode or service instance configuration mode. To disable SNMP link trap generation, use the **no** form of this command.

snmp trap link-status [**permit**]
no snmp trap link-status

Syntax Description

permit	(Optional) Permits SNMP linkup and linkdown traps.

Command Default

SNMP link trap status is the default.

Command Modes

Interface configuration (config-if)

Service instance configuration (config-if-srv)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE snmp trap link-status command.

Examples

The following example shows how to disable SNMP link traps related to the ISDN BRI interface 0:

```
Device(config)# interface bri 0
Device(config-if)# no snmp trap link-status
```

The following example shows how to enable SNMP link traps for service instance 50 on Ethernet interface 0/1:

```
Device(config)# interface virtual-template 1
Device(config-if)# service instance 50 ethernet
Device(config-if-srv)# snmp trap link-status
```

tftp-server

To configure a router or a Flash memory device on the router as a TFTP server, use one of the following **tftp-server** commands in global configuration mode. This command replaces the **tftp-server system** command. To remove a previously defined filename, use the **no** form of this command with the appropriate filename.

tftp-server bootflash *bootflash-filename*
no tftp-server bootflash

Syntax Description

bootflash	Specifies TFTP service of a file in Flash memory.
bootflash-filename	Name of a file in Flash or in ROM that the TFTP server uses in answering TFTP Read Requests.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates

Usage Guidelines

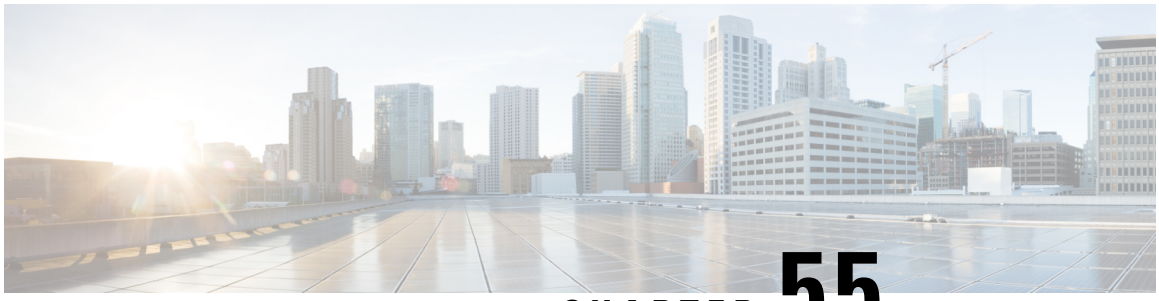
You can specify multiple filenames by repeating the **tftp-server** command. The system sends a copy of the system image contained in ROM or one of the system images contained in Flash memory to any client that issues a TFTP Read Request with this filename.

If the specified *bootflash-filename1*or *bootflash-filename2*argument exists in Flash memory, a copy of the Flash image is sent. On systems that contain a complete image in ROM, the system sends the ROM image if the specified *bootflash-filename1*or *bootflash-filename2*argument is not found in Flash memory.

Examples

In the following example, the command **tftp-server bootflash:***c2900-universalk9-mz.SPA.154-3.M3.bin* configures a Cisco IOS XE Catalyst SD-WAN device to act as a TFTP server, making the specified IOS image file (c2900-universalk9-mz.SPA.154-3.M3.bin) located in its bootflash: memory available for other network devices to download.

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# tftp-server bootflash:c2900-universalk9-mz.SPA.154-3.M3.bin
```



CHAPTER 55

SSL Proxy Commands

- sslproxy, on page 811
- sslproxy ca-tp-label, on page 812
- sslproxy certificate-lifetime, on page 813
- sslproxy eckey-type, on page 814
- sslproxy enable, on page 815
- sslproxy rsa-key-modulus, on page 816
- sslproxy settings certificate-revocation-check, on page 817
- sslproxy settings expired-certificate, on page 818
- sslproxy settings failure-mode, on page 819
- sslproxy settings minimum-tls-ver, on page 820
- sslproxy settings unknown-status, on page 821
- sslproxy settings untrusted-certificate, on page 823
- sslproxy settings unsupported-cipher-suites, on page 824
- sslproxy settings unsupported-protocol-versions, on page 825

sslproxy

To enter the sslproxy configuration mode, use the **sslproxy** command in global configuration mode. This command does not have a **no** form.

sslproxy

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

A typical SSL handshake involves authentication using certificates signed by trusted, third-party Certificate Authorities (CAs). TLS is the successor of SSL although is sometimes still referred to as SSL. This command can be used to enter the sslproxy configuration mode where further configurations can be done.

Example

The following example shows how to enter the sslproxy configuration mode.

```
Device(config)# sslproxy
```

Table 46: Related Commands

Command	Description
ca-cert-bundle	Filename of CA certificate bundle.
ca-tp-label	Default Trustpoint label for SSL Proxy.
certificate-lifetime	Certificate lifetime in days.
eckey-type	EC key type for SSL Proxy.
enable	Enables SSL Proxy.
rsa-key-modulus	RSA key length.
settings	Advanced settings for SSL Proxy.

sslproxy ca-tp-label

To set the Default Trustpoint label for SSL proxy, use the **ca-tp-label** command in sslproxy configuration mode. To reset the default Trustpoint label for SSL proxy to the default label of PROXY-SIGNING-CA, use the **no** form of this command.

ca-tp-label *label*
no ca-tp-label

Syntax Description

label	Name of the label <string, Minimum characters: 1, Maximum characters: 128>.

Command Default

Default Trustpoint label is PROXY-SIGNING-CA.

Command Modes

SSL Proxy configuration (config-sslproxy).

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

SSL proxy devices act as man-in-the-middle (MitM) to decrypt encrypted SSL traffic traveling across WAN, and send it to UTD for inspection. The Trustpoint label is a name for the RSA key pair. Use this **ca-tp-label** command to set the default Trustpoint label for SSL proxy.

Example

The following example shows how to set the default Trustpoint label for SSL proxy to NEW-PROXY-CA.

```
Device(config)# sslproxy
Device(config-sslproxy)# ca-tp-label NEW-PROXY-CA
```

Table 47: Related Commands

Command	Description
ca-cert-bundle	Filename of CA certificate bundle.
certificate-lifetime	Certificate lifetime in days.
eckey-type	EC key type for SSL proxy.
enable	Enables SSL proxy.
rsa-key-modulus	RSA key length.
settings	Advanced settings for SSL Proxy.

sslproxy certificate-lifetime

To set the lifetime of the proxy certificate, use the **certificate-lifetime** command in sslproxy configuration mode. To reset the lifetime of the proxy certificate to the default value, use the **no** form of this command.

certificate-lifetime *value*
no certificate-lifetime

Syntax Description

value	Sets the lifetime of the proxy certificate in days. The range is from 1 to 4294967295.

Command Default

Default value is 730 (days).

Command Modes

SSL Proxy configuration (config-sslproxy).

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Once you configure a Certificate Authorities (CA) for SSL proxy, the CA issues signing certificates to the SSL proxy device. The device then securely stores the subordinate CA keys, and dynamically generates and signs the proxy certificates. Use this **certificate-lifetime** command to set the lifetime of the proxy certificate.

Example

The following example shows how to set the lifetime of the proxy certificate to 365 days.

```
Device(config)# sslproxy
Device(config-sslproxy)# certificate-lifetime 365
```

Table 48: Related Commands

Command	Description
ca-cert-bundle	Filename of CA certificate bundle.
ca-tp-label	Default Trustpoint label for SSL proxy.
eckey-type	EC key type for SSL proxy.
enable	Enables SSL Proxy.
rsa-key-modulus	RSA key length.
settings	Advanced settings for SSL proxy.

sslproxy eckey-type

To set the elliptic curve cryptography key type for SSL proxy, use the **eckey-type** command in sslproxy configuration mode. To reset the elliptic curve cryptography key type to the default value of P256, use the **no** form of this command.

eckey-type { **P256** | **P384** | **P521** }
no eckey-type

Syntax Description

P256	Specifies the EC key type to P256.
P384	Specifies the EC key type to P384.
P521	Specifies the EC key type to P521.

Command Default

The default value is P256.

Command Modes

SSL Proxy configuration (config-sslproxy).

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. One of the main benefits in comparison with non-ECC cryptography is

the same level of security provided by keys of smaller size. Larger keys offer stronger security but takes longer to use. Use this **eckey-type** command to set the EC key type.

Example

The following example shows how to set the EC key type to P521.

```
Device(config)# sslproxy
Device(config-sslproxy)# eckey-type P521
```

Table 49: Related Commands

Command	Description
ca-cert-bundle	Filename of CA certificate bundle.
ca-tp-label	Default Trustpoint label for SSL proxy.
certificate-lifetime	Certificate lifetime in days.
enable	Enables SSL proxy.
rsa-key-modulus	RSA key length.
settings	Advanced settings for SSL proxy.

sslproxy enable

To enable SSL proxy, use the **enable** command in sslproxy configuration mode. To disable SSL proxy, use the **no** form of this command.

enable
no enable

Syntax Description

This command has no keywords or arguments.

Command Default

SSL proxy is not enabled.

Command Modes

SSL proxy configuration (config-sslproxy).

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

SSL proxy devices act as man-in-the-middle (MitM) to decrypt encrypted SSL traffic traveling across WAN, and send it to UTD for inspection. SSL proxy thus allows devices to identify risks that are hidden by end-to-end encryption over SSL channels. The data is re-encrypted post inspection before being sent to its final destination. TLS is the successor of SSL, although, it is sometimes still referred to as SSL. Use this **enable** command to enable SSL proxy.

Example

The following example shows how to enable SSL proxy.

```
Device(config)# sslproxy
Device(config-sslproxy)# enable
```

Table 50: Related Commands

Command	Description
ca-cert-bundle	Filename of CA certificate bundle.
ca-tp-label	Default Trustpoint label for SSL proxy.
certificate-lifetime	Certificate lifetime in days.
eckey-type	EC key type for SSL proxy.
rsa-key-modulus	RSA key length.
settings	Advanced settings for SSL proxy.

sslproxy rsa-key-modulus

To set the rsa-key-modulus key size, use the **rsa-key-modulus** command in sslproxy configuration mode. To reset the rsa-key-modulus to the default key size of 2048, use the **no** form of this command.

rsa-key-modulus *key size*
no rsa-key-modulus

Syntax Description

key size	Specifies the key size. Range: 1024 to 4096.

Command Default

The default key size is 2048.

Command Modes

SSL proxy configuration (config-sslproxy).

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

The command can be used to set the rsa-key-modulus key size. The longer the modulus, the stronger the security. However, a longer modulus takes longer to generate and to use.

Example

The following example shows how to set the rsa-key-modulus key size to 4096.

```
Device(config)# sslproxy
Device(config-sslproxy)# rsa-key-modulus 4096
```

Table 51: Related Commands

Command	Description
ca-cert-bundle	Filename of CA certificate bundle.
ca-tp-label	Default Trustpoint label for SSL proxy.
certificate-lifetime	Certificate lifetime in days.
eckey-type	EC key type for SSL proxy.
enable	Enables SSL proxy.
settings	Advanced settings for SSL proxy.

sslproxy settings certificate-revocation-check

To change the sslproxy certificate-revocation-check setting, use the **settings certificate-revocation-check** command in sslproxy configuration mode. To reset the sslproxy certificate-revocation-check setting to the default value of none, use the **no** form of this command.

settings certificate-revocation-check { **none** | **ocsp** }
no settings certificate-revocation-check

Syntax Description

none	Disables certificate revocation checking.
ocsp	Specifies that the method Online Certificate Status Protocol (OCSP) be used to check the revocation status of the server certificate.

Command Default

Default setting is none.

Command Modes

SSL proxy configuration (config-sslproxy).

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

A typical SSL handshake involves authentication using certificates signed by trusted, third-party Certificate Authorities. TLS is the successor of SSL, although, it is sometimes still referred to as SSL. Use the **settings certificate-revocation-check** command to set the method the SSL proxy uses to check the certificate status.

Example

The following example show how to set OSCP as the method for SSL proxy to use to check the certificate status.

```
Device(config)# sslproxy
Device(config-sslproxy)# settings certificate-revocation-check ocsp
```

Table 52: Related Commands

Commands	Description
expired-certificate	Specifies the action for expired certificate.
failure-mode	Specifies the action for failure mode.
minimum-tls-ver	Specifies the minimum TLS version for SSL proxy.
unknown-status	Specifies the action for unknown status.
unsupported-cipher-suites	Specifies the action for unsupported cipher suite.
unsupported-protocol-versions	Specifies the action for unsupported protocol version.
untrusted-certificate	Specifies the action for untrusted certificate.

sslproxy settings expired-certificate

To change the sslproxy expired-certificate setting, use the **settings expired-certificate** command in sslproxy configuration mode. To reset the sslproxy expired-certificate setting to the default value of drop, use the **no** form of this command.

settings expired-certificate { **decrypt** | **drop** }
no settings expired-certificate

Syntax Description

decrypt	The packet is forwarded to the client and goes through the following: • TCP optimization for optimization of traffic • Decryption of encrypted traffic through TLS proxy • Threat inspection through UTD • Re-encryption of decrypted traffic through TLS proxy
drop	The hello packet from the client is dropped and the connection is reset.

Command Default

The default setting is dropped.

Command Modes

SSL proxy configuration (config-sslproxy).

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

A typical SSL handshake involves authentication using certificates signed by trusted, third-party Certificate Authorities (CAs). TLS is the successor of SSL although is sometimes still referred to as SSL. Use this **settings expired-certificate** command to set the action the SSL proxy should do if the server certificate is expired.

Example

The following example shows how to set the action to decrypt the encrypted traffic if the server certificate has expired.

```
Device(config)# sslproxy
Device(config-sslproxy)# settings expired-certificate decrypt
```

Table 53: Related Commands

Commands	Description
certificate-revocation-check	Specifies ocsp or none.
failure-mode	Specifies action for failure mode.
minimum-tls-ver	Specifies minimum TLS version for SSL proxy.
unknown-status	Specifies action for unknown status.
unsupported-cipher-suites	Specifies action for unsupported cipher suite.
unsupported-protocol-versions	Specifies action for unsupported protocol version.
untrusted-certificate	Specifies action for untrusted certificate.

sslproxy settings failure-mode

To change the sslproxy failure-mode setting, use the **settings failure-mode** command in sslproxy configuration mode. To reset the sslproxy failure-mode setting to the default value of close, use the **no** form of this command.

settings failure-mode { **close** | **open** }
no settings failure-mode

Syntax Description

close	Specifies the failure mode to close.
open	Specifies the failure mode to open.

Command Default

The default setting is close.

Command Modes

SSL proxy configuration (config-sslproxy).

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

A typical SSL handshake involves authentication using certificates signed by trusted, third-party Certificate Authorities (CAs). TLS is the successor of SSL, although, it is sometimes still referred to as SSL. Use this **settings failure-mode** command to set the failure mode when the SSL handshake fails.

Example

The following example shows how to set the failure mode when the SSL handshake fails to open.

```
Device(config)# sslproxy
Device(config-sslproxy)# settings failure-mode open
```

Table 54: Related Commands

Commands	Description
certificate-revocation-check	Specifies ocsp or none.
expired-certificate	Specifies action for expired certificate.
minimum-tls-ver	Specifies minimum TLS version for SSL proxy.
unknown-status	Specifies action for unknown status.
unsupported-cipher-suites	Specifies action for unsupported cipher suite.
unsupported-protocol-versions	Specifies action for unsupported protocol version.
untrusted-certificate	Specifies action for untrusted certificate.

sslproxy settings minimum-tls-ver

To change the sslproxy minimum-tls-ver setting, use the **settings minimum-tls-ver** command in sslproxy configuration mode. To reset the sslproxy minimum-tls-ver setting to the default value of TLSv1, use the **no** form of this command.

settings minimum-tls-ver { **TLSv1** | **TLSv1.1** | **TLSv1.2** }
no settings minimum-tls-ver

Syntax Description

TLSv1	Specifies the minimum supported TLS version as 1.
TLSv1.1	Specifies the minimum supported TLS version as 1.1.
TLSv1.2	Specifies the minimum supported TLS version as 1.2.

Command Default

The default setting is TLSv1.

Command Modes SSL proxy configuration (config-sslproxy).

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines A typical SSL handshake involves authentication using certificates signed by trusted, third-party Certificate Authorities. TLS is the successor of SSL, although, it is sometimes still referred to as SSL. Use the **settings minimum-tls-ver** command to set the minimum supported TLS version.

Example

The following example shows how to set the minimum supported TLS version to TLSv1.2.

```
Device(config)# sslproxy
Device(config-sslproxy)# settings minimum-tls-ver tlsv1.2
```

Table 55: Related Commands

Commands	Description
certificate-revocation-check	Specifies OCSP or none.
expired-certificate	Specifies the action for expired certificate.
failure-mode	Specifies the action for failure mode.
unknown-status	Specifies the action for unknown status.
unsupported-cipher-suites	Specifies the action for unsupported cipher suite.
unsupported-protocol-versions	Specifies the action for unsupported protocol version.
untrusted-certificate	Specifies the action for untrusted certificate.

sslproxy settings unknown-status

To change the sslproxy unknown-status setting, use the **settings unknown-status** command in sslproxy configuration mode. To reset the sslproxy unknown-status setting to the default value of drop, use the **no** form of this command.

settings unknown-status { **decrypt** | **drop** }
no settings unknown-status

Syntax Description

decrypt	The packet is forwarded to the client and goes through the following: • TCP optimization for optimization of traffic. • Decryption of encrypted traffic through TLS proxy. • Threat inspection through Unified Threat Defense (UTD). • Re-encryption of decrypted traffic through TLS proxy.
drop	The hello packet from the client is dropped and the connection is reset.

Command Default

The default setting is drop.

Command Modes

SSL proxy configuration (config-sslproxy).

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

A typical SSL handshake involves authentication using certificates signed by trusted, third-party Certificate Authorities. TLS is the successor of SSL although is sometimes still referred to as SSL. Use the **settings unknown-status** command to set the action the SSL proxy should do if the server certificate status is unknown.

Example

The following example shows how to set the action to decrypt the encrypted traffic if the server certificate status is unknown.

```
Device(config)# sslproxy
Device(config-sslproxy)# settings unknown-status decrypt
```

Table 56: Related Commands

Commands	Description
certificate-revocation-check	Specifies OCSP or none.
expired-certificate	Specifies the action for expired certificate.
failure-mode	Specifies the action for failure mode.
minimum-tls-ver	Specifies the minimum TLS version for SSL proxy.
unsupported-cipher-suites	Specifies the action for unsupported cipher suite.
unsupported-protocol-versions	Specifies the action for unsupported protocol version.
untrusted-certificate	Specifies the action for untrusted certificate.

sslproxy settings untrusted-certificate

To change the sslproxy untrusted-certificate setting, use the **settings untrusted-certificate** command in sslproxy configuration mode. To reset the setting to default value of drop, use the **no** form of this command.

settings untrusted-certificate { **decrypt** | **drop** }
no settings untrusted-certificate

Syntax Description

decrypt	The packet is forwarded to the client and goes through the following: • TCP optimization for optimization of traffic • Decryption of encrypted traffic through TLS proxy • Threat inspection through UTD • Re-encryption of decrypted traffic through TLS proxy
drop	The hello packet from the client is dropped and the connection is reset.

Command Default

The default setting is drop.

Command Modes

SSL Proxy configuration (config-sslproxy)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

A typical SSL handshake involves authentication using certificates signed by trusted, third-party Certificate Authorities (CAs). TLS is the successor of SSL although it is sometimes still referred to as SSL. Use this **settings untrusted-certificate** command to set the action, the SSL proxy should do if the server certificate is untrusted.

Example

The following example shows how to set the action to decrypt the encrypted traffic if the server certificate is untrusted.

```
Device(config)# sslproxy
Device(config-sslproxy)# settings untrusted-certificate decrypt
```

Table 57: Related Commands

Commands	Description
certificate-revocation-check	Specifies ocsp or none.
expired-certificate	Specifies action for expired certificate.
failure-mode	Specifies action for failure mode.

Commands	Description
minimum-tls-ver	Specifies minimum TLS version for SSL proxy.
unknown-status	Specifies action for unknown status.
unsupported-cipher-suites	Specifies action for unsupported cipher suite.
unsupported-protocol-versions	Specifies action for unsupported protocol version.

sslproxy settings unsupported-cipher-suites

To change the sslproxy unsupported-cipher-suites setting, use the **settings unsupported-cipher-suites** command in sslproxy configuration mode. To reset the sslproxy unsupported-cipher-suites setting to the default value of drop, use the **no** form of this command.

settings unsupported-cipher-suites { **drop** | **no-decrypt** }
no settings unsupported-cipher-suites

Syntax Description

drop	The hello packet from the client is dropped and the connection is reset.
no-decrypt	The hello packet from the client bypasses the SSL proxy.

Command Default

The default setting of this command is drop.

Command Modes

SSL proxy configuration (config-sslproxy).

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

A typical SSL handshake involves authentication using certificates signed by trusted, third-party Certificate Authorities (CAs). TLS is the successor of SSL, although, it is sometimes still referred to as SSL. The SSL Proxy feature in Cisco Catalyst SD-WAN only supports certain cipher suites. Use this **settings unsupported-cipher-suites** command to set the action the SSL proxy should do if the cipher suite detected is unsupported.

Example

The following example shows how to set the action to no-decrypt if the cipher suite detected is unsupported.

```
Device(config)# sslproxy
Device(config-sslproxy)# settings unsupported-cipher-suites no-decrypt
```

Table 58: Related Commands

Commands	Description
certificate-revocation-check	Specifies ocsp or none.
expired-certificate	Specifies action for expired certificate.
failure-mode	Specifies action for failure mode.
minimum-tls-ver	Specifies minimum TLS version for SSL proxy.
unknown-status	Specifies action for unknown status.
unsupported-protocol-versions	Specifies action for unsupported protocol version.
untrusted-certificate	Specifies action for untrusted certificate.

sslproxy settings unsupported-protocol-versions

To change the sslproxy unsupported-protocol-versions setting, use the **settings unsupported-protocol-versions** command in sslproxy configuration mode. To reset the sslproxy unsupported-protocol-versions setting to the default value of drop, use the **no** form of this command.

settings unsupported-protocol-versions { **drop** | **no-decrypt** }
no settings unsupported-protocol-versions

Syntax Description

drop	The hello packet from the client is dropped and the connection is reset.
no-decrypt	The hello packet from the client bypasses SSL proxy.

Command Default

The default setting is drop.

Command Modes

SSL proxy configuration (config-sslproxy).

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

A typical SSL handshake involves authentication using certificates signed by trusted, third-party Certificate Authorities. TLS is the successor of SSL, although, it is sometimes still referred to as SSL. The SSL proxy can be set to require a minimum TLS protocol version. Use the **settings unsupported-protocol-versions** command to set the action the SSL proxy should do if the protocol version detected is unsupported.

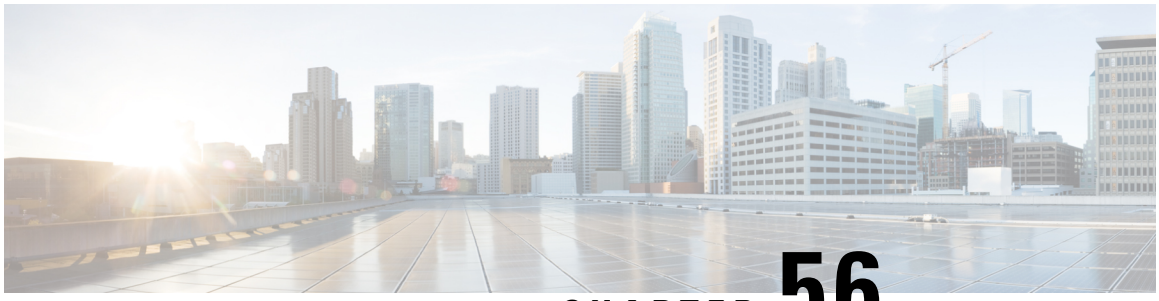
Example

The following example shows how to set the action to no-decrypt if the protocol version detected is unsupported.

```
Device(config)# sslproxy
Device(config-sslproxy)# settings unsupported-protocol-versions no-decrypt
```

Table 59: Related Commands

Commands	Description
certificate-revocation-check	Specifies OCSP or none.
expired-certificate	Specifies the action for expired certificate.
failure-mode	Specifies the action for failure mode.
unknown-status	Specifies the action for unknown status.
minimum-tls-ver	Specifies the minimum TLS version for SSL proxy.
unsupported-cipher-suites	Specifies the action for unsupported cipher suite.
untrusted-certificate	Specifies the action for untrusted certificate.



CHAPTER 56

System Commands

- admin-tech-on-failure (system), on page 827
- console-baud-rate, on page 828
- control-session-pps (system), on page 829
- controller-group-list (system), on page 829
- device-groups (system), on page 830
- enable-ipv6-unique-local-address , on page 830
- gps-location (system), on page 831
- logging, on page 834
- max-omp-sessions (system), on page 836
- organization-name (system), on page 837
- overlay-id (system), on page 837
- port-hop (system), on page 838
- port-offset (system), on page 839
- site-id (system), on page 839
- sp-organization-name (system), on page 840
- statistics table interface collection-interval, on page 841
- system-ip (system), on page 841
- system overlay-id, on page 842
- track-transport (system), on page 843
- track-default-gateway (system), on page 843
- upgrade-confirm (system), on page 844
- vbond (system), on page 845

admin-tech-on-failure (system)

When a Cisco device reboots, it collects system status information in a compressed tar file to aid in troubleshooting and diagnostics. This tar file, which is saved in the user's home directory, contains the output of various commands and the contents of various files on the local device, including syslog files, files for each process (daemon) running on the device, core files, and configuration rollback files. For aid in troubleshooting, send the tar file to Cisco customer support.

To configure a device to collect system status information in an admin-tech file when the device reboots, use the **admin-tech-on-failure** command in system configuration mode. To delete the system status information from the admin tech file, use the no form of this command.

admin-tech-on-failure

no admin-tech-on-failure

Syntax Description

This comand has no keywords or arguments.

Command Modes

system configuration (config-system)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Examples

The following example configures the device to collect system status information in an admin-tech file when the device reboots:

```
Router(config)# system
Router(config-system)# admin-tech-on-failure
!
```

console-baud-rate

To change the baud rate of the console connection on a Cisco IOS XE Catalyst SD-WAN device, use the **console-baud-rate** command in system configuration mode. To delete the configured baud rate, use the **no** form of this command.

console-baud-rate *rate*

no console-baud-rate

Syntax Description

rate	Specifies the baud rate, in baud or bits per second (bps). Each signal carries only one bit, so the baud rate is equal to the bits-per-second rate. Values: 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 Starting from Cisco vManage Release 20.3.1, the default value is 9600 on Cisco IOS XE Catalyst SD-WAN devices.

Command Modes

system configuration (config-system)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Examples

The following example changes the console baud rate to 57600:

```
Device(config)# system
Device(config-system)# console-baud-rate 57600
```

control-session-pps (system)

To police the flow of DTLS control session traffic, use the **control-session-pps** command in system configuration mode. To delete the control session traffic rate, use the no form of this command.

control-session-pps *site-id*

no control-session-pps

Syntax Description

rate	Sets the maximum rate of DTLS control session traffic in packets per second (pps). Range: 1 - 65535 pps Default: 300 pps

Command Modes

system configuration (config-system)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Examples

The following example changes the maximum control session traffic rate to 250 pps:

```
Router(config)# system
Router(config-system)# control-session-pps 250
```

controller-group-list (system)

To list the controller groups to which a router belongs, use the **controller-group-list** command in system configuration mode. A router can form control connections only with the Cisco Catalyst SD-WAN Controllers that are in the same controller group. To delete the control connections from the Cisco Catalyst SD-WAN Controllers, use the no form of this command.

controller-group-list *list-of-controller-groups*

no controller-group-list *list-of-controller-groups*

Syntax Description

list-of-controller-groups	Specifies an identifier of one or more Cisco Catalyst SD-WAN Controllerr groups to which a router belongs. You configure this identifier on the Cisco Catalyst SD-WAN Controllers, using the **system controller-group-id** command. The number of controller groups cannot exceed the maximum number of control connections configured on the router.

Command Modes

system configuration (config-system)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Examples

The following example allows a router to establish control connections to the Cisco Catalyst SD-WAN Controllers in groups 1 and 2:

```
Router(config)# system
Router(config-system)# controller-group-list 1 2
```

device-groups (system)

To configure one or more groups to which a device belongs, use the **device-groups** command in system configuration mode. To delete the groups to which a device belongs, use the no form of this command.

device-groups *group-name*

no device-groups *group-name*

Syntax Description

group-name	Name of one or more groups to which the device belongs. When specifying multiple group names, enclose the names in square brackets. When a group name contains spaces, enclose it in quotation marks (" ").

Command Modes

system configuration (config-system)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Examples

The following example adds a router to two groups: London and the United Kingdom:

```
Router(config)# system
Router(config-system)# device-groups London ["United Kingdom"]
```

enable-ipv6-unique-local-address

To enable the IPv6 Unique Local Addresses (ULA), use the **enable-ipv6-unique-local-address** command in system configuration mode. To disable these addresses, use the no form of this command.

enable-ipv6-unique-local-address

no enable-ipv6-unique-local-address

Command Modes

system configuration (config-system)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Examples

The following example enables the IPv6 Unique Local Address:

```
Router(config)# system
Router(config-system)# enable-ipv6-unique-local-address
```

gps-location (system)

To configure the location and the geofencing boundary for a device and to enable SMS alerts for boundary violations, use the **gps-location** command in system configuration mode. To disable geofencing, use the **no** form of this command.

gps-location [**latitude** *decimal-number*] [**longitude** *decimal-number*] [**auto-detect-geofencing-location**] [**geo-fencing-enable** [**geo-fencing-config** [**geo-fencing-range** *meters*] [**sms** [[**sms-enable**] **mobile-number** *mobile-number*]]]]

no gps-location

Syntax Description

latitude *decimal-number*	(Optional) Specifies the latitude coordinates of a device in decimal degrees. Range: -90.0 - 90.0 **Note** For configuring the **gps-location** command for geofencing, the **latitude**, **longitude**, and **geo-fencing-enable** parameters are mandatory. Although the syntax allows you to configure **latitude**, **longitude**, and **geo-fencing-enable** parameters in separate **gps-location** commands, we recommend that all three be configured within a single command. All three have to be configured with **geo-fencing-enable** configured last. A single command reduces the risk of configuration errors by keeping corequisite parameters close together, and single-command syntax ensures that **geo-fencing-enable** is configured last. **Note** Deconfigure the **latitude**, **longitude**, and **geo-fencing-enable** parameters by using the **no gps-location** command. You can configure a maximum of six digits to the right of the decimal point.

longitude *decimal-number*	(Optional) Specifies the longitude coordinates of a device in decimal degrees. Range: -180.0 - 180.0 **Note** For configuring the **gps-location** command for geofencing, the **latitude**, **longitude**, and **geo-fencing-enable** parameters are mandatory. Although the syntax allows you to configure **latitude**, **longitude**, and **geo-fencing-enable** parameters in separate **gps-location** commands, we recommend that all three be configured within a single command. All three have to be configured with **geo-fencing-enable** configured last. A single command reduces the risk of configuration errors by keeping corequisite parameters close together, and single-command syntax ensures that **geo-fencing-enable** is configured last. **Note** Deconfigure the **latitude**, **longitude**, and **geo-fencing-enable** parameters by using the **no gps-location** command. You can configure a maximum of six digits to the right of the decimal point.
auto-detect-geofencing-location	(Optional) Enables automatic detection of a device where the device determines its own location. You can choose either to specify latitude and longitude parameters, or configure the **auto-detect-geofencing-location** parameter. **Note** Do not configure latitude and longitude coordinates when enabling **auto-detect-geofencing-location**. This field allows you to configure geofencing with the last-known valid GPS coordinates of the device, instead of mandating latitude and longitude coordinates for GPS location. The last-known GPS coordinates are persistent across boot cycles and are periodically updated as the location of the device changes. If no historically valid last-known GPS coordinates are available, the device rejects the automatic detection configuration.
geo-fencing-config	(Optional) Allows you to configure geofencing parameters.
geo-fencing-range *meters*	(Optional) Specifies the radius from the base target location in meters. Default geofencing range is 100 meters. Configurable ranges of values is 100 to 10,000 meters.
sms	(Optional) Provides SMS notification options.

sms-enable	(Optional) Enables registration of end-user mobile numbers for receiving SMS alerts. An SMS alert is delivered when a device is determined to be outside the configured geofencing radius of its target location. **Note** The presence of a SIM card is mandatory in the LTE PIM module for receiving SMS alerts.
mobile-number *mobile-number*	(Optional) Specifies the mobile numbers for sending SMS alerts. Mobile numbers must start with a + sign, include a country code, an area code, with no spaces between the country code and the area code, and the remaining digits. You can configure a maximum of four mobile numbers for receiving SMS alerts.

Command Modes

system configuration (config-system)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Additional parameters qualified: • **geo-fencing enable** • **geo-fencing config** • **geo-fencing range** • **sms** • **sms-enable** • **mobile-number**
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	Additional parameter qualified: **auto-detect-geofencing-location**

Usage Guidelines

Note In Cisco IOS XE Catalyst SD-WAN Release 17.6.1a and earlier releases, geofencing parameters such as, **latitude**, **longitude**, and **geo-fence range** are not reconfigurable once configured. You need to first disable geofencing and then reenable geofencing again with the updated parameters.

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.7.1a, **latitude**, **longitude**, and **geo-fence range** are all reconfigurable.

Provide **latitude** and **longitude** coordinates as close as possible to the intended installation location of the device. This is necessary because of inherent inaccuracies of GPS and fluctuations over time.

Whenever there are too many **Device Location Inside** and **Device Location Outside** notifications generated for the device on Cisco SD-WAN Manager when the device is in a static installation environment, we suggest picking a higher value for the **geo-fence-range** parameter to account for GPS fluctuations.

Examples

The following examples set the geographical coordinates of a device:

```
Device(config)# system
Device(config-system)# gps-location latitude 37.317342 longitude -122.218170
```

```
Device(config)# system
Device(config-system)# gps-location longitude 91.1 latitude 11.0
```

The following example shows enabling and configuring geofencing with a geofence range of 1000 meters.

```
Device(config-system)# gps-location geo-fencing-enable
Device(config-system)# gps-location geo-fencing-config
Device(conf-geo-fencing-config)# geo-fencing-range 1000
```

The following example shows enabling SMS and adding a mobile number for receiving SMS alerts.

```
Device(conf-geo-fencing-config)# sms sms-enable mobile-number +1214343789
Device(config-mobile-number-+1214343789)#
```

The following example shows configuring a device without the **auto-detect-geofencing-location** parameter:

```
Device(config)# system
Device(config-system)# gps-location latitude 37.439917 longitude -121.886471
```

You need to configure latitude and longitude coordinates when not enabling the **auto-detect-geofencing-location** parameter.

The following example shows enabling a device using the **auto-detect-geofencing-location** parameter:

```
Device(config)# system
Device(config-system)# no gps-location latitude
Device(config-system)# no gps-location longitude
Device(config-system)# gps-location auto-detect-geofencing-location
```

You should not configure latitude and longitude coordinates when enabling the **auto-detect-geofencing-location** parameter.

logging

To set system logging parameters use the **logging** command in global configuration mode. To remove logging parameters, use the **no** form of this command.

logging { **IP address** | **console** | **event** | **host** | **persistent** | **tls-profile** | **string** | **discriminator** | **file** | **monitor** | **snmp-trap** | **trap** | **buffered** | **esm** | **history** | **origin-id** | **source-interface** }
no logging { **IP address** | **console** | **event** | **host** | **persistent** | **tls-profile** | **string** | **discriminator** | **file** | **monitor** | **snmp-trap** | **trap** | **buffered** | **esm** | **history** | **origin-id** | **source-interface** }

Syntax Description

ip address	IP address of the host that will receive the system logging (syslog) messages.

console	Limits messages logged to the console. By default, the console receives debugging messages and numerically lower levels.
event	Logs interface events.
host	Logs messages to a UNIX syslog server host.
persistent	Allows writing logged messages to files on the routers flash disk.
tls-profile	Profile used for secure syslog messages with TLSv1.1 or TLSv1.2.
string	Includes the custom string in the session ID tag. Custom string in the s_id="custom_string" tag.
discriminator	(Optional) Specifies a message discriminator for the session. Name of the message discriminator.
file	Stores log messages in a file in flash memory on a standalone switch or, a switch stack, on the active switch.
monitor	Limits messages logged to the terminal lines. By default, the terminal receives debugging messages and numerically lower levels.
snmp-trap	Logs SNMP-trap notifications.
trap	Limits messages logged to the syslog servers. By default, syslog servers receive informational messages and numerically lower levels.
buffered	Logs messages to an internal buffer on the switch or on a standalone switch or, a switch stack, on the active switch.
esm	syslog filter modules, which are Tool Command Language (Tcl) script files stored locally or on a remote device.
history	Changes the default level of syslog messages stored in the history file and sent to the SNMP server. By default, warnings, errors, critical, alerts, and emergencies messages are sent.
origin-id	Adds an origin identifier to system logging messages sent to remote hosts.
source-interface	Specifies the source IPv4 or IPv6 address of system logging packets.

Command Default

Logging to the console is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Logging events can be configured and stored on local flash of router or sent out via syslog or snmp-trap.

Example

The following example shows setting the TLS-version of profile1 to TLSv1.1

```
Device(config)# logging tls-profile profile1 tls-version TLSv1.1
```

The following example shows how to log interface events

```
Device(config)# logging event link-status default
```

max-omp-sessions (system)

To configure the maximum number of OMP sessions that a device can establish with Cisco Catalyst SD-WAN Controllers, use the **max-omp-sessions** command in system configuration mode.

max-omp-sessions *number*

Syntax Description

name	Specifies the maximum number of OMP sessions that a device can establish with Cisco Catalyst SD-WAN Controllers. These connections are DTLS or TLS control plane tunnels. Range: 0–100

Command Modes

system configuration (config-system)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

A Cisco IOS XE Catalyst SD-WAN device establishes a single OMP session with each Cisco Catalyst SD-WAN Controller. Even when a device has multiple tunnel connections with the same Cisco Catalyst SD-WAN Controller, because all the tunnels have the same IP address, this group of tunnels is effectively a single OMP session. When **max-omp-sessions** is configured (without affinity), the devices establish OMP peering with Cisco Catalyst SD-WAN Controllers having higher System-IP.

In an overlay network with redundant Cisco Catalyst SD-WAN Controllers, configure the maximum number of OMP sessions to manage the scale of the overly network, by limiting the number of Cisco Catalyst SD-WAN Controllers that an individual device can establish control connections with.

This command provides system-wide control over the maximum number of control connections that a device can establish to Cisco Catalyst SD-WAN Controllers. To configure the number of control connections allowed on an individual tunnel interface, include the **max-control-connections** command when configuring the tunnel interface in VPN 0. The maximum number of OMP sessions configured on the router becomes the default value for the maximum number of control connections allowed on the tunnel interfaces of a device.

Examples

The following example changes the maximum number of Cisco Catalyst SD-WAN Controller connections to 8:

```
Router(config)# system
Router(config-system)# max-omp-sessions 8
```

organization-name (system)

To configure the name of your organization, use the **organization-name** command in system configuration mode. To delete the organization name configuration, use the no form of this command.

organization-name *name*

no organization-name

Syntax Description

name	Configures the name of your organization. The name is case-sensitive. It must be identical on all the devices in your overlay network, and it must match the name in the certificates for all Cisco IOS XE Catalyst SD-WAN devices.

Command Modes

system configuration (config-system)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Starting from Cisco Catalyst SD-WAN Manager Release 20.15.1, the size limit of the organization name must be within the range 1 to 128.

Examples

The following example configures an organization name:

```
Router(config)# system
Router(config-system)# organization-name Cisco
```

overlay-id (system)

To configure the overlay id of a device in Cisco SD-WAN overlay netowrk, use the **overlay-id** command in system configuration mode. To delete the overlay id, use the no form of this command.

overlay-id *overlay-id*

no overlay-id

Syntax Description

overlay-id	Specifies the overlay id of a device. Range: Range: 0 - 4294967295 (2^{32} – 1) Default: 1

Command Modes

system configuration (config-system)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Examples

The following example sets the overlay Id of a device:

```
Router(config)# system
Router(config-system)# overlay-id 42000
```

port-hop (system)

To establish DTLS connections with other Cisco IOS XE Catalyst SD-WAN devices when a connection attempt is unsuccessful (on Cisco IOS XE Catalyst SD-WAN devices, Cisco SD-WAN Manager servers, and Cisco Catalyst SD-WAN Controllers), use the **port-hop** command in system configuration mode. To disable port hopping on the Cisco IOS XE Catalyst SD-WAN device, or if global port hopping is enabled, to disable port hopping on an individual TLOC, use the no form of this command.

port-hop

no port-hop

Syntax Description

This comand has no keywords or arguments.

Command Modes

system configuration (config-system)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For a Cisco IOS XE Catalyst SD-WAN device that is behind a NAT device or for an individual tunnel interface (TLOC) on the device, rotate through a pool of preselected OMP port numbers, known as base ports. By default, port hopping is enabled on Cisco IOS XE Catalyst SD-WAN devices and on all tunnel interfaces on Cisco IOS XE Catalyst SD-WAN devices, and it's disabled on Cisco SD-WAN Manager servers and Cisco Catalyst SD-WAN Controllers.

There are five base ports: 12346, 12366, 12386, 12406, and 12426. These port numbers determine the ports used for connection attempts. The first connection attempt is made on port 12346. If the first connection doesn't succeed after about 1 minute, port 12366 is tried. After about 2 minutes, port 12386 is tried; after about 5 minutes, port 12406; after about 6 minutes, port 12426 is tried. Then the cycle returns to port 12346.

If you have configured a port offset with the **port-offset** command, the five base ports are a function of the configured offset. For example, with a port offset of 2, the five base ports are 12348, 12368, 12388, 12408, and 12428. Cycling through these base ports happens in the same way as if you hadn't configured an offset.

Examples

The following example enables port hopping:

```
Router(config)# system
Router(config-system)# port-hop
!
```

port-offset (system)

To offset the base port numbers to be used for the TLOC when multiple Cisco devices are present behind a single NAT device, use the **port-offset** command in system configuration mode. Each device must have a unique port number so that overlay network traffic can be correctly delivered. To delete the port offset value, use the no form of this command.

port-offset *number*

no port-offset

Syntax Description

number	Specifies offset value from the default base port numbers, which are 12346, 12366, 12386, 12406, and 12426. Range: 0-19 Default: 0

Command Modes

system configuration (config-system)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Examples

The following example configures a port offset value:

```
Router(config)# system
Router(config-system)# port-offset 1
```

site-id (system)

To configure the identifier of a site in the Cisco SD-WAN overlay network, such as a branch, campus, or data center, in which devices and controllers reside, use the **site-id** command in system configuration mode. To delete the site id of a device, use the no form of this command.

site-id *site-id*

no site-id

Syntax Description

site-id	Numeric identifier of the site in the Cisco SD-WAN overlay network. The site ID must be the same for all routers that reside in the same site. Range: 0 - 4294967295 (2^{32} – 1) Default: 101

Command Modes

system configuration (config-system)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Examples

The following example configures the site id of a device to 50:

```
Router(config)# system
Router(config-system)# site-id 50
```

sp-organization-name (system)

To configure the name of your service provider for a Cisco Catalyst SD-WAN Validator or Cisco Catalyst SD-WAN Controller that is part of a software multitenant architecture, use the **sp-organization-name** command in system configuration mode. To delete the service provider organization name configuration, use the no form of this command.

sp-organization-name *name*

no sp-organization-name

Syntax Description

name	Configures the name of your service provider. The name is case-sensitive. It must be identical on all the devices in your overlay network, and it must match the name in the certificates for all Cisco IOS XE Catalyst SD-WAN devices.

Command Modes

system configuration (config-system)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.15.1a, the size limit of the organization name must be within the range 1 to 128.

Examples

The following example configures a service provider organization name:

```
Router(config)# system
Router(config-system)# sp-organization-name My Phone Company Inc
```

statistics table interface collection-interval

To set the interface statistics collection interval in Cisco IOS XE Catalyst SD-WAN, use the **statistics table interface collection-interval** command in global configuration mode.

statistics table interface collection-interval *interval-time*

Syntax Description

interval-time	Specify the data collection interval for interface statistics as 1 (minute).

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 26.1.1	This command was introduced.

Examples

The following is an example of how to set the interface statistics collection interval on a WAN edge device:

```
Device(config)# statistics
Device(config-statistics)# table interface
Device(config-table-interface)# collection-interval 1
```

system-ip (system)

To configure a system IP address of a device, use the **system-ip** command in system configuration mode. To delete the system IP address of a device, use the no form of this command.

system-ip *ipv4-address*

no system-ip

Syntax Description

ipv4-address	Specifies an IPv4 address in decimal four-part dotted notation. Enter the address, and the prefix length (/32) is implicit. The system IP address can be any IPv4 address except for 0.0.0.0/8, 127.0.0.0/8, 224.0.0.0/4, 240.0.0.0/4 and later. Each device in the overlay network must have a unique system IP address. You can't use the same address for another interface in VPN 0.

Command Modes

system configuration (config-system)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

The system IP address is a persistent IP address that identifies the Cisco device. It's similar to a router ID on a regular router, which is the address used to identify the router from which packets originated. The system IP address is used internally as the loopback address of the device in the transport VPN (VPN 0).



Note This IP address isn't the same as a loopback address that you configure for an interface.

On a router, the system IP address is used as the router ID for BGP or OSPF. If you configure a router ID for either of these protocols and it's different from the system IP address, the router ID takes precedence.

Examples

The following example sets the system IP address of a device:

```
Router(config)# system
Router(config-system)# system-ip 172.16.255.11
```

system overlay-id

To set an overlay-id, use the **system overlay-id** command in global configuration mode. To remove the overlay-id, use the **no** form of this command.

system overlay-id *ID*
no system overlay-id *ID*

Syntax Description

ID	Specifies the ID number 0-4294967295.

Command Default

Default overlay-id is set to 1.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

The overlay-id command is used to determine whether devices belong to specific SD-WAN topologies or overlay.

Example

The following example shows how to configure an overlay-id of 2335.

```
Device(config)# system overlay-id 2335
```

track-transport (system)

To check whether the routed path between the local device and a Cisco Catalyst SD-WAN Validator is available by using ICMP probes at regular interval of 3s, use the **track-transport** command in system configuration mode. To delete the regular monitoring of the DTLS connection to the Cisco Catalyst SD-WAN Validator, use the no form of this command. By default, transport checking is enabled.

track-transport

no track-transport

Syntax Description

This comand has no keywords or arguments.

Command Modes

system configuration (config-system)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Examples

The following example explicitly configures regular monitoring of the DTLS connection to the Cisco Catalyst SD-WAN Validator:

```
Router(config)# system
Router(config-system)# track-transport
Router(config-system)# commit
Commit complete.
```

track-default-gateway (system)

For a static default route, to determine whether the next hop is reachable before adding that route to the device's route table, use the **track-default-gateway** command in system configuration mode. To disable the device from determining whether the next hop for a default static route is reachable before placing the deafault static route in the local route table, use the no form of the command. By default, this command is enabled.

track-default-gateway

no track-default-gateway

Syntax Description

This comand has no keywords or arguments.

Command Modes

system configuration (config-system)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

With gateway tracking enabled, the software sends ARP messages every 10 seconds to the next hop of a default static route. If the software receives an ARP response, it places the default static route into the local route table. After 10 consecutive ARP responses are missed, the default static route is removed from the route table. The software continues to periodically send ARP messages, and as soon as it once again receives an ARP responses, the default static route is added back to the route table.

Examples

The following example configures the device to determine whether the next hop for a default static route is reachable before placing the static route in the local route table:

```
Router(config)# system
Router(config-system)# track-default-gateway
```

upgrade-confirm (system)

To configure the time limit for confirming that a software upgrade is successful, use the **upgrade-confirm** command in system configuration mode. It's recommended that you configure this on all Cisco IOS XE Catalyst SD-WAN devices. To disable the time limit configuration set for successful software upgrade, use the no form of this command.

upgrade-confirm *minutes*

no upgrade-confirm

Syntax Description

minutes	Specifies how long to wait for the **request software sdwan upgrade-confirm** command to be issued before reverting to the previous software image if a software upgrade fails. Range: 5-60 minutes Default: None

Command Modes

system configuration (config-system)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

By default, software upgrade confirmation isn't enabled. When you enable the confirmation, the device waits for the amount of time you configure. If the device doesn't get booted up within that time, the device reverts to the previous image.

When the upgrade-confirm is enabled, the devices can still revert to the previous image if the control-connections fail to boot up.

After you issue the **request software sdwan software install** command to upgrade the software and then log in to the device after the reboot completes, enter the **request software sdwan upgrade-confirm** command within the configured time limit to confirm that the software upgrade is successful. If you do not, the system automatically reverts to the previous software image.

Examples

The following example sets the upgrade confirmation time to 5 minutes:

After a software upgrade, when the system reboots and restarts, if you don't issue a **request software sdwan upgrade-confirm** command within 5 minutes (either from the CLI or from the Cisco SD-WAN Manager), the system automatically reverts to the software image that was running before the upgrade:

```
Router(config)# system
Router(config-system)# upgrade-confirm 5
!
```

vbond (system)

To configure the IP address and other information related to the Cisco Catalyst SD-WAN Validator, use the **vbond** command in system configuration mode. To remove the Cisco Catalyst SD-WAN Validator configuration from the device, use the no form of this command.

vbond *dns-name ip-address* [**local**] [**port** *port-number*] [**ztp-server**]

no vbond [**local**] [**port** *port-number*]

Syntax Description

dns-name	Specifies the DNS name that points to a Cisco Catalyst SD-WAN Validator or to a number of Cisco Catalyst SD-WAN Validators. The addresses can be resolved to Cisco Catalyst SD-WAN Validators configured with IPv4 addresses, IPv6 addresses, or with both IPv4 and IPv6 adresses.
ip-address	Specifies IPv4 or IPv6 address of the Cisco Catalyst SD-WAN Validator, in decimal four-part dotted notation. You can configure one IP address, and it must be a public IP address.
local	Designates the Cisco IOS XE Catalyst SD-WAN device to be a Cisco Catalyst SD-WAN Validator in the overlay network domain. If you configure the **local** option, you can omit the DNS name, or IP address of the Cisco Catalyst SD-WAN Validator as long as one of the interfaces in VPN 0 has a routable public IP address.
port-number	Specifies the port number to use to connect to the Cisco Catalyst SD-WAN Validator. If you omit this option, the local system first tries port 12346 on the Cisco Catalyst SD-WAN Validator. If this port is not available, the system then tries port 12366 and then port 12388, rotating through these three port numbers until one is available. If you do not want to rotate through these three port numbers, configure the port number to connect to the Cisco Catalyst SD-WAN Validator. Range: 1-65535 Default: 12346
ztp-server	Designates the local Cisco IOS XE Catalyst SD-WAN device to be the zero-touch-provisioning (ZTP) server in the overlay network domain. Such a Cisco Catalyst SD-WAN Validator acts as an enterprise ZTP server, and provides the devices in your domain with the IP address of your enterprise Cisco Catalyst SD-WAN Validator and with the enterprise root CA chain. You must load two files onto your enterprise ZTP server–the authorized serial number file of the device that you received and your enterprise root CA chain, which must be signed by Symantec.

Command Modes

system configuration (config-system)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

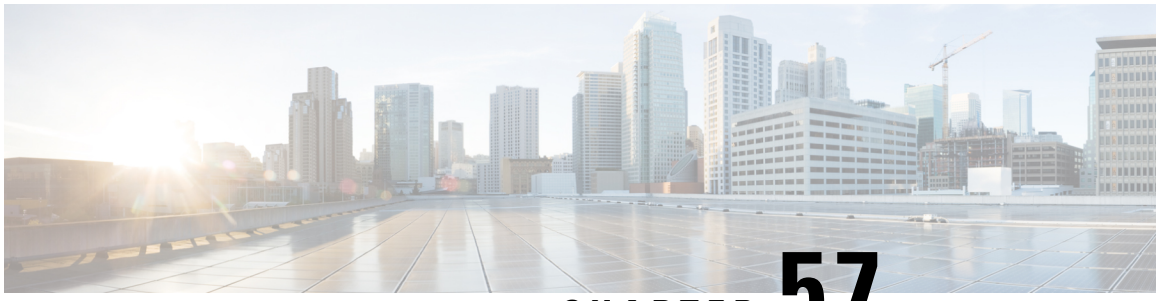
Usage Guidelines

If you have configured an IP address for the Cisco Catalyst SD-WAN Validator, to change the address, you must delete the address and then configure the new address. Doing this causes all the existing device connections to the other devices in the network to go down. The devices come back up after you commit the configuration with the new IP address. To avoid this problem, we recommend that you always use a DNS name for your Cisco Catalyst SD-WAN Validators, and then make changes to the DNS devices instead of on the Cisco IOS XE Catalyst SD-WAN devices and Cisco Catalyst SD-WAN Controllers directly.

Examples

The following example configures the port number of a device used to connect to the Cisco Catalyst SD-WAN Validator:

```
Router(config)# system
Router(config-system)# vbond 192.0.2.4 port 12346
```



CHAPTER 57

TCP Commands

Instructions for TCP Commands

Note Some configurations and protocols are identified as insecure and is a security risk for Cisco devices. Existing deployments continue to function, but new installations require intentional enablement. For more information on remediation, refer to Resilient Infrastructure: Cisco Catalyst SD-WAN and Routing

- service tcp-keepalives-in, on page 847
- service tcp-keepalives-out, on page 848
- service tcp-small-servers, on page 848
- service udp-small-servers, on page 849

service tcp-keepalives-in

To generate keepalive packets on idle incoming network connections (initiated by the remote host), use the **service tcp-keepalives-in** command in global configuration mode . To disable the keepalives, use the **no**form of this command.

service tcp-keepalives-in
no service tcp-keepalives-in

Syntax Description This command has no arguments or keywords.

Command Default Disabled

Command Modes Global configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Command qualified for use in Cisco vManage CLI templates.

Examples In the following example, keepalives on incoming TCP connections are generated:

```
Device(config)# service tcp-keepalives-in
```

service tcp-keepalives-out

To generate keepalive packets on idle outgoing network connections (initiated by a user), use the **service tcp-keepalives-out** command in global configuration mode . To disable the keepalives, use the **no**form of this command.

service tcp-keepalives-out
no service tcp-keepalives-out

Syntax Description This command has no arguments or keywords.

Command Default Disabled

Command Modes Global configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Command qualified for use in Cisco vManage CLI templates.

Examples

In the following example, keepalives on outgoing TCP connections are generated:

```
Device(config)# service tcp-keepalives-out
```

service tcp-small-servers

To enable small TCP servers such as the Echo, use the **service tcp-small-servers** command in global configuration mode. To disable the TCP server, use the **no** form of this command.

service tcp-small-servers
no service tcp-small-servers

Command Default TCP small servers are disabled.

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE service tcp small servers command.

Examples

The following example shows how to enable small TCP servers:

```
Device(config)# service tcp-small-servers
```

service udp-small-servers

To enable small User Datagram Protocol (UDP) servers such as the Echo, use the **service udp-small-servers** command in global configuration mode. To disable the UDP server, use the **no** form of this command.

service udp-small-servers
no service udp-small-servers

Command Default

UDP small servers are disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Command qualified for use in Cisco vManage CLI templates.

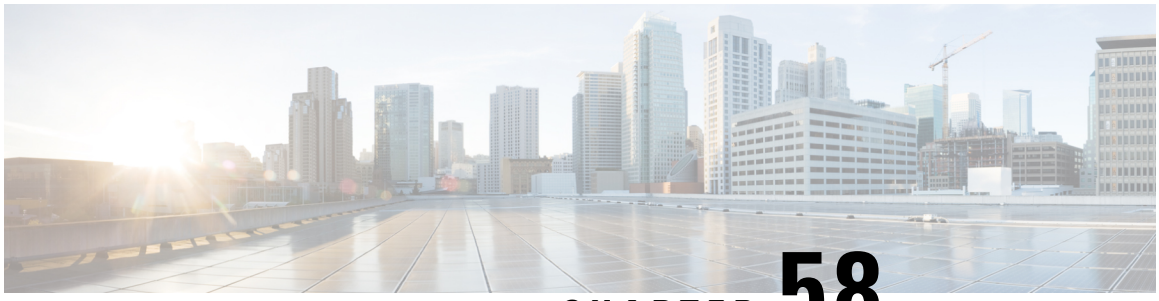
Usage Guidelines

For usage guidelines, see the Cisco IOS XE service udp small servers command.

Examples

The following example shows how to enable small UDP:

```
Router(config)# service udp-small-servers
```



CHAPTER 58

Tracker Commands

- boolean, on page 851
- endpoint-api-url, on page 853
- endpoint-dns-name, on page 853
- endpoint-ip, on page 854
- endpoint-tracker, on page 855
- endpoint-tracker-settings, on page 856
- Endpoint Tracker SLA Profile, on page 857
- interval, on page 857
- icmp-interval, on page 858
- multiplier, on page 859
- threshold, on page 860
- tracker-elements, on page 861
- tracker-type, on page 862

boolean

To enable boolen logic while configuring a tracker group, use the **boolean** command in endpoint tracker configuration mode. To disable boolean logic, use the **no** form of this command.

boolean { **and** | **or** }
no boolean { **and** | **or** }

Syntax Description

{and | or}	Specifies boolean AND or OR logic that is used to configure a tracker group. OR logic ensures that the endpoint status is reported as active if either one of the associated trackers of the tracker group report that the endpoint is active. AND logic ensures that the endpoint status is reported as active if both the associated trackers of the tracker group report that the endpoint is active.

Command Default

OR is enabled.

Command Modes

Endpoint-tracker configuration (config-endpoint-tracker)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

Tracker boolean is set to OR as default.

A tracker group can have a mix of endpoint trackers. For example, to create a static route group, you can combine an IP address tracker and a TCP/UDP tracker. Similarly, to create a NAT Direct Internet Access (DIA) tracker group, you can combine an IP address tracker and a DNS tracker. You can apply only one tracker to a static route endpoint.

Examples

The following example shows how to configure a tracker group with two static route trackers (two endpoints) using the tracker boolean AND or OR:

```
Device(config)# endpoint-tracker tcp-10001
Device(config-endpoint-tracker)# tracker-type static-route
Device(config-endpoint-tracker)# endpoint-ip 10.1.1.1 tcp 10001
Device(config-endpoint-tracker)# threshold 100
Device(config-endpoint-tracker)# multiplier 10
Device(config-endpoint-tracker)# interval 1
Device(config-endpoint-tracker)# exit
Device(config)# track tcp-10001 endpoint-tracker

Device(config)# endpoint-tracker udp-10002
Device(config-endpoint-tracker)# tracker-type static-route
Device(config-endpoint-tracker)# endpoint-ip 10.2.2.2 udp 10002
Device(config-endpoint-tracker)# threshold 100
Device(config-endpoint-tracker)# multiplier 5
Device(config-endpoint-tracker)# interval 2
Device(config)# track udp-10002 endpoint-tracker
Device(config-endpoint-tracker)# exit

Device(config)# endpoint-tracker static-route-group
Device(config-endpoint-tracker)# tracker-type tracker-group
Device(config-endpoint-tracker)# tracker-elements tcp-10001 udp-10002
Device(config-endpoint-tracker)# boolean and

Device(config)# track static-route-group endpoint-tracker
Device(config-endpoint-tracker)# exit
```

The following example shows how to configure tracker groups using boolean logic to probe NAT DIA interface:

```
Device(config)# endpoint-tracker tracker1
Device(config-endpoint-tracker)# tracker-type interface
Device(config-endpoint-tracker)# endpoint-ip 10.1.1.1
Device(config-endpoint-tracker)# threshold 100
Device(config-endpoint-tracker)# multiplier 10
Device(config-endpoint-tracker)# interval 1
Device(config-endpoint-tracker)# exit
Device(config)# endpoint-tracker tracker2
Device(config-endpoint-tracker)# tracker-type interface
Device(config-endpoint-tracker)# endpoint-dns-name www.diatracker.com
Device(config-endpoint-tracker)# threshold 1000
Device(config-endpoint-tracker)# multiplier 10
Device(config-endpoint-tracker)# interval 600
Device(config-endpoint-tracker)# exit
```

```
Device(config)# endpoint-tracker group1
Device(config-endpoint-tracker)# tracker-type tracker-group
Device(config-endpoint-tracker)# tracker-elements tracker1 tracker2
Device(config-endpoint-tracker)# boolean or
Device(config-endpoint-tracker)# exit
```

endpoint-api-url

To configure the API URL of an endpoint, use the **endpoint-api-url** command in endpoint tracker configuration mode. To diable API URL configuration, use the **no** form of this command.

endpoint-api-url *url-address*
no endpoint-api-url *url-address*

Syntax Description

url-address	API URL of an endpoint. This is the destination in the internet to which the router sends probes to determine the status of the endpoint.

Command Default

If endpoint-api-url is not configured, tracker is disabled.

Command Modes

Endpoint-tracker configuration (config-endpoint-tracker)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Examples

The following example shows how to configure an API URL:

```
Device(config)# endpoint-tracker tracker1

Device(config-endpoint-tracker)# endpoint-api-url http://gateway.zscalerbeta.net/vpntest
```

endpoint-dns-name

To configure the domain system name of an endpoint, use the **endpoint-dns-name** command in endpoint tracker configuration mode. To disable the configuration, use the **no** form of this command.

endpoint-dns-name *dns-name*
no endpoint-dns-name *dns-name*

Syntax Description

dns-name	DNS name of the endpoint. This is the destination on the internet to which probes are sent to determine the status of the endpoint. DNS name can contain a minimum of 1 character and a maximum of 253 characters.

Command Default

If endpoint-dns-name is not configured, tracker is disabled.

Command Modes Endpoint-tracker configuration (config-endpoint-tracker)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Examples

The following example shows how to configure the DNS name:

```
Device(config)# endpoint-tracker tracker1

Device(config-endpoint-tracker)# endpoint-dns-name www.cisco.com
```

The following example shows how to configure a DNS name for the NAT DIA interface:

```
Device(config)# endpoint-tracker tracker2
Device(config-endpoint-tracker)# endpoint-dns-name www.diatracker.com
Device(config-endpoint-tracker)# tracker-type interface
```

endpoint-ip

To configure the IP address of an endpoint, use the **endpoint-ip** command in endpoint tracker configuration mode. To disable the configuration, use the **no** form of this command.

Syntax for Static Route Endpoint

endpoint-ip *ip-address* [**tcp** *port-number* | **udp** *port-number*]
no endpoint-ip *ip-address* [**tcp** *port-number* | **udp** *port-number*]

Syntax for NAT DIA Interface

endpoint-ip *ip-address*
no endpoint-ip *ip-address*

Syntax Description

ip-address	IP address of an endpoint. This is the destination on the internet to which the probes are sent to determine the status of an endpoint.
tcp *port-number*	TCP endpoint type for static route.
udp *port-number*	UDP endpoint type for static route.

Command Default If endpoint-ip is not configured, the commit CLI fails.

Command Modes Endpoint-tracker configuration (config-endpoint-tracker)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Examples

The following example shows how to configure a static route tracker with TCP port endpoint:

```
Device(config)# endpoint-tracker tcp-10001
Device(config-endpoint-tracker)# tracker-type static-route
Device(config-endpoint-tracker)# endpoint-ip 10.0.0.1 tcp 10001
Device(config-endpoint-tracker)# threshold 100
Device(config-endpoint-tracker)# interval 10
Device(config-endpoint-tracker)# multiplier 1
Device(config-endpoint-tracker)# exit
Device(config)# track tcp-10001 endpoint-tracker
Device(config-track)# ip route vrf 1 192.168.0.0 255.255.0.0 10.1.19.16 100 track name
tcp-10001
```

The following example shows how to configure a static route tracker with UDP port endpoint:

```
Device(config)# endpoint-tracker udp-10002
Device(config-endpoint-tracker)# tracker-type static-route
Device(config-endpoint-tracker)# endpoint-ip 10.0.0.1 udp 10002
Device(config-endpoint-tracker)# threshold 100
Device(config-endpoint-tracker)# interval 10
Device(config-endpoint-tracker)# multiplier 1
Device(config-endpoint-tracker)# exit
Device(config)# track udp-10002 endpoint-tracker
Device(config-track)# ip route vrf 1 192.168.0.0 255.255.0.0 10.1.19.16 100 track name
udp-10002
```

The following example shows how to configure a NAT DIA tracker with IPv4 endpoint:

```
Device(config)# endpoint-tracker tracker1
Device(config-endpoint-tracker)# tracker-type interface
Device(config-endpoint-tracker)# endpoint-ip 10.0.0.1
Device(config-endpoint-tracker)# threshold 100
Device(config-endpoint-tracker)# multiplier 5
Device(config-endpoint-tracker)# interval 20
Device(config-endpoint-tracker)# exit
```

endpoint-tracker

To configure the endpoint tracker for tracking the status of an endpoint, use the **endpoint-tracker** command in global configuration mode. To disable the endpoint tracker, use the **no** form of this command.

endpoint-tracker *tracker-name*
no endpoint-tracker *tracker-name*

Syntax Description

tracker-name	Tracker name. You can enter up to 128 characters.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

You can apply only one tracker to an endpoint.

Examples

The following example shows how to configure a single static-route tracker:

```
Device(config)# endpoint-tracker tracker1
Device(config-endpoint-tracker)# tracker-type static-route
Device(config-endpoint-tracker)# endpoint-ip 10.1.1.1
Device(config-endpoint-tracker)# threshold 100
Device(config-endpoint-tracker)# multiplier 1
Device(config-endpoint-tracker)# interval 10
Device(config-endpoint-tracker)# exit
```

The following example shows how to configure a single NAT DIA tracker:

```
Device(config)# endpoint-tracker tracker1
Device(config-endpoint-tracker)# tracker-type interface
Device(config-endpoint-tracker)# endpoint-ip 10.1.1.1
Device(config-endpoint-tracker)# threshold 100
Device(config-endpoint-tracker)# multiplier 5
Device(config-endpoint-tracker)# interval 20
Device(config-endpoint-tracker)# exit
```

endpoint-tracker-settings

To configure the endpoint tracker settings for HTTP and ICMP trackers to stabilize the tracker states and avoid interface flaps while tracking the status of an endpoint, use the **endpoint-tracker-settings** command in global configuration mode. To disable the endpoint tracker, use the **no** form of this command.

endpoint-tracker-settings [**dia-stabilize-status** | **name-lookup-over-sig**]
no endpoint-tracker-settings [**dia-stabilize-status** | **name-lookup-over-sig**]

Syntax Description

dia-stabilize-status	Statibilizes the interface flaps by using the multiplier to update tracker status from DOWN to UP. For tracker groups, if you use boolean AND, the tracker element which comes up last will trigger the group UP. In case of boolean OR, the tracker element that comes UP first triggers the tracker UP.
name-lookup-over-sig	Controls where DNS probes for endpoint-tracker on SIG tunnels go in to the tunnel or underlay interface.

Command Default

Endpoint Stability status is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.13.1a	This command was introduced.

Examples

The following example shows how to configure the endpoint tracker settings to stabilize the tracker status changes:

```
Device(config)# endpoint-tracker-settings dia-stabilize-status

Device(config)# endpoint-tracker-settings name-lookup-over-sig
```

Endpoint Tracker SLA Profile

To configure the end point tracker for SLA profile, use the **endpoint-tracker-sla-profile** command in global configuration mode. To disable the configuration, use the **no** form of this command.

endpoint-tracker-sla-profile *profile-name* [**jitter** *jitter-value* | **latency** *latency-value* | **loss** *loss-value* | **sla-mode** { *aggressive* | *moderate* | *conservative* }]

Syntax Description

profile-name	Specify the profile name.
loss	Specify packet loss value in percentage.
latency	Specify latency value in milliseconds.
jitter	Specify jitter value as milliseconds.
sla-mode	Specify SLA mode.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.14.1a	This command was introduced.

The following example shows how to configure an end point tracker for SLA profile:

```
Device(config)# endpoint-tracker-sla-profile sla_agg
Device(config)#loss 10
Device(config)# latency 300
Device(config)# jitter 80
Device(config)# sla-mode aggressive
```

interval

To set the interval period, in seconds, in which probes are sent to determine the status of an endpoint, use the **interval** command in endpoint tracker configuration mode. To revert to the default setting, use the **no** form of this command.

interval *interval-value*
no interval *interval-value*

Syntax Description

interval-value	Time interval, in seconds, in which probes are sent to determine the status of the endpoint. Range: 20 to 600. Default: 60.

Command Default

Interval is configured with a default value of 60 seconds.

Command Modes

Endpoint-tracker configuration (config-endpoint-tracker)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Examples

The following example shows how to configure an interval of 10 secs between the probes used to track a TCP endpoint:

```
Device(config)# endpoint-tracker tcp-10001
Device(config-endpoint-tracker)# tracker-type static-route
Device(config-endpoint-tracker)# endpoint-ip 10.0.0.1 tcp 10001
Device(config-endpoint-tracker)# threshold 100
Device(config-endpoint-tracker)# interval 10
Device(config-endpoint-tracker)# multiplier 1
Device(config-endpoint-tracker)# exit
```

The following example shows how to configure an interval of 10 secs between the probes used to track an NAT DIA endpoint:

```
Device(config)# endpoint-tracker tracker1
Device(config-endpoint-tracker)# tracker-type interface
Device(config-endpoint-tracker)# endpoint-ip 10.1.1.1
Device(config-endpoint-tracker)# threshold 100
Device(config-endpoint-tracker)# interval 10
Device(config-endpoint-tracker)# multiplier 1
Device(config-endpoint-tracker)# exit
```

icmp-interval

To set the interval period, in seconds, in which ICMP probes are sent to determine the status of an ICMP endpoint teacker, use the **icmp-interval** command in endpoint tracker configuration mode. To revert to the default setting, use the **no** form of this command.

icmp-interval *interval-value*
no icmp-interval *interval-value*

Syntax Description

interval-value	Time interval, in seconds, in which probes are sent to determine the status of the endpoint. Range: 2 to 1000. Default: 2.

Command Default ICMP probe interval is configured with a default value of two seconds.

Command Modes Endpoint-tracker configuration (config-endpoint-tracker)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.13.1a	This command was introduced.

Examples

The following example shows how to configure an interval of 10 secs between the probes used to track an ICMP endpoint:

```
Device(config)# endpoint-tracker tracker1
Device(config-endpoint-tracker)# tracker-type interface-icmp
Device(config-endpoint-tracker)# endpoint-ip 10.0.0.1
Device(config-endpoint-tracker)# threshold 100
Device(config-endpoint-tracker)# icmp-interval 10
Device(config-endpoint-tracker)# multiplier 1
Device(config-endpoint-tracker)# exit
```

For more information about configuring the ICMP endpoint tracker interval, see the section ICMP Endpoint Tracker for NAT DIA in *ICMP Endpoint Tracker for NAT DIA*.

Related Commands

Commands	Description
tracker-type	Specifies the tracker type for an individual tracker.
tracker-group	Specifies tracker-type as tracker group to configure a tracker group with dual endpoints.
interface-icmp	Specifies the interface type as an ICMP interface.

multiplier

To configure the multiplier that defines the number of retries required to resend probes before declaring that the endpoint is inactive, use the **multiplier** command in endpoint tracker configuration mode. To revert to the default value, use the **no** form of this commad.

multiplier *multiplier-value*
no multiplier *multiplier-value*

Syntax Description

multiplier-value	Required number of times to resend probes before declaring that the endpoint is inactive. Range: 1 to 10. Default: 3

Command Default None

Command Modes Endpoint-tracker configuration (config-endpoint-tracker)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Examples

The following example shows how to configure a multiplier value of 2 for an UDP port endpoint:

```
Device(config)# endpoint-tracker udp-10001
Device(config-endpoint-tracker)# tracker-type static-route
Device(config-endpoint-tracker)# endpoint-ip 10.0.0.1 udp 10001
Device(config-endpoint-tracker)# multiplier 2
Device(config-endpoint-tracker)# exit
Device(config)# track udp-10001 endpoint-tracker
```

The following example shows how to configure a multiplier value of 5 for a NAT DIA endpoint:

```
Device(config)# endpoint-tracker tracker
Device(config-endpoint-tracker)# tracker-type interface
Device(config-endpoint-tracker)# endpoint-ip 10.1.1.1
Device(config-endpoint-tracker)# multiplier 5
Device(config-endpoint-tracker)# exit
```

threshold

To set the threshold time required to wait for the probe to return a response before declaring that the endpoint is inactive, use the **threshold** command in endpoint tracker configuration mode. To revert to the default value, use the **no** form of this command.

threshold *threshold-value*
no threshold *threshold-value*

Syntax Description

threshold-value	Time required to wait for the probe to return a response before declaring that the endpoint is inactive. Range: 100 to 1000. Default: 300.

Command Default

None

Command Modes

Endpoint-tracker configuration (config-endpoint-tracker)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Examples

The following example shows how to configure a threshold of value 100 for a static route with an UDP port endpoint:

```
Device(config)# endpoint-tracker udp-10001
```

```
Device(config-endpoint-tracker)# tracker-type static-route
Device(config-endpoint-tracker)# endpoint-ip 10.0.0.1 udp 10001
Device(config-endpoint-tracker)# threshold 100
Device(config-endpoint-tracker)# exit
```

The following example shows how to configure a threshold of value 100 for an NAT DIA endpoint:

```
Device(config)# endpoint-tracker tracker
Device(config-endpoint-tracker)# tracker-type interface
Device(config-endpoint-tracker)# endpoint-ip 10.1.1.1
Device(config-endpoint-tracker)# threshold 100
Device(config-endpoint-tracker)# exit
```

tracker-elements

To add tracker names to create a dual endpoint tracker group, use the **tracker-elements** command in endpoint-tracker (tracker-group) configuration mode. To disable the configuration, use the **no** form of this command.

tracker-elements *tracker1 tracker2*
no tracker-elements *tracker1 tracker2*

Syntax Description

tracker1 *tracker2*	Tracker names to be included while creating a tracker group. Add the existing tracker names (separated by a space). When you add trackers to the template, the tracker group is associated with these individual trackers. You can then associate the tracker group to an endpoint.

Command Default

None

Command Modes

Endpoint-tracker configuration (tracker-group)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

only a maximum of two tracker endpoints can be added in a tracker group.

A tracker group can have a mix of endpoint trackers. For example, to create a static route group, you can combine an IP address tracker and a TCP/UDP tracker. Similarly, to create a NAT DIA tracker group, you can combine an IP address tracker and a DNS tracker. You can apply only one tracker to a static route endpoint.

Examples

The following example shows how to configure a tracker group with two static route endpoints:

```
Device(config)# endpoint-tracker tcp-10001
Device(config-endpoint-tracker)# tracker-type static-route
Device(config-endpoint-tracker)# endpoint-ip 10.1.1.1 tcp 10001
Device(config-endpoint-tracker)# threshold 100
Device(config-endpoint-tracker)# multiplier 10
Device(config-endpoint-tracker)# interval 1
Device(config-endpoint-tracker)# exit
```

```
Device(config)# track tcp-10001 endpoint-tracker

Device(config)# endpoint-tracker udp-10002
Device(config-endpoint-tracker)# tracker-type static-route
Device(config-endpoint-tracker)# endpoint-ip 10.2.2.2 udp 10002
Device(config-endpoint-tracker)# threshold 100
Device(config-endpoint-tracker)# multiplier 5
Device(config-endpoint-tracker)# interval 2
Device(config)# track udp-10002 endpoint-tracker
Device(config-endpoint-tracker)# exit

Device(config)# endpoint-tracker static-route-group
Device(config-endpoint-tracker)# tracker-type tracker-group
Device(config-endpoint-tracker)# tracker-elements tcp-10001 udp-10002
Device(config-endpoint-tracker)# boolean and

Device(config)# track static-route-group endpoint-tracker
Device(config-endpoint-tracker)# exit
```

The following example shows how to configure a tracker group with two NAT DIA endpoints:

```
Device(config)# endpoint-tracker tracker1
Device(config-endpoint-tracker)# tracker-type interface
Device(config-endpoint-tracker)# endpoint-ip 10.1.1.1
Device(config-endpoint-tracker)# threshold 100
Device(config-endpoint-tracker)# multiplier 10
Device(config-endpoint-tracker)# interval 1
Device(config-endpoint-tracker)# exit

Device(config)# endpoint-tracker tracker2
Device(config-endpoint-tracker)# tracker-type interface
Device(config-endpoint-tracker)# endpoint-dns-name www.diatracker.com
Device(config-endpoint-tracker)# threshold 1000
Device(config-endpoint-tracker)# multiplier 10
Device(config-endpoint-tracker)# interval 600
Device(config-endpoint-tracker)# exit

Device(config)# endpoint-tracker group1
Device(config-endpoint-tracker)# tracker-type tracker-group
Device(config-endpoint-tracker)# tracker-elements tracker1 tracker2
Device(config-endpoint-tracker)# boolean or
Device(config-endpoint-tracker)# exit
```

tracker-type

To configure the tracker type for an individual tracker and to configure the tracker type for a tracker group, use the **tracker-type** command in endpoint tracker configuration mode. To disable the configurations, use the **no** form of this command.

tracker-type [**interface** | **ipv6-interface** | **static-route** | **tracker-group** | **interface-icmp** | **ipv6-interface-icmp**]
no tracker-type [**interface** | **ipv6-interface** | **static-route** | **tracker-group** | **interface-icmp** | **ipv6-interface-icmp**]

Syntax Description

interface	Specifies tracker-type as interface to configure endpoint trackers. Default tracker-type is interface.

ipv6-interface	Specifies tracker-type as as an IPv6 interface to configure endpoint trackers.
static-route	Specifies tracker-type as static-route to configure endpoint trackers.
tracker-group	Specifies tracker-type as tracker group to configure a tracker group with dual endpoints. From Cisco IOS XE Catalyst SD-WAN Release 17.7.1a, you can configure a tracker group with dual endpoints in Cisco IOS XE Catalyst SD-WAN devices, and associate this tracker group to an endpoint.
interface-icmp	Tracks an IPv4 interface via ICMP probes.
ipv6-interface-icmp	Tracks an IPv6 interface via ICMP probes.

Command Default

Interface type is enabled.

Command Modes

Endpoint-tracker configuration (config-endpoint-tracker)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.
Cisco IOS XE Catalyst SD-WAN Release 17.13.1a	New keywords were added to this command: • interface-icmp • ipv6-interface-icmp

Usage Guidelines

A tracker group can have a mix of endpoint trackers. For example, to create a static route group, you can combine an IP address tracker and a TCP/UDP tracker. Similarly, to create a NAT DIA tracker group, you can combine an IP address tracker and a DNS tracker. Note that you can apply only one tracker to a static route endpoint.

Examples

The following example shows how to configure tracker type as static-route for a tracker with a TCP endpoint:

```
Device(config)# endpoint-tracker tcp-10001
Device(config-endpoint-tracker)# tracker-type static-route
Device(config-endpoint-tracker)# endpoint-ip 10.1.1.1 tcp 10001
Device(config-endpoint-tracker)# threshold 100
Device(config-endpoint-tracker)# multiplier 10
Device(config-endpoint-tracker)# interval 1
Device(config-endpoint-tracker)# exit
Device(config)# track tcp-10001 endpoint-tracker
```

The following example shows how to configure tracker type as tracker-group for creating a tracker group with dual static-route endpoints:

```
Device(config)# endpoint-tracker tcp-10001
Device(config-endpoint-tracker)# tracker-type static-route
Device(config-endpoint-tracker)# endpoint-ip 10.1.1.1 tcp 10001
Device(config-endpoint-tracker)# multiplier 10
Device(config-endpoint-tracker)# exit
Device(config)# track tcp-10001 endpoint-tracker
```

```
Device(config)# endpoint-tracker udp-10002
Device(config-endpoint-tracker)# tracker-type static-route
Device(config-endpoint-tracker)# endpoint-ip 10.2.2.2 udp 10002
Device(config-endpoint-tracker)# threshold 100
Device(config-endpoint-tracker)# interval 2
Device(config-endpoint-tracker)# exit
Device(config)# track udp-10002 endpoint-tracker

Device(config)# endpoint-tracker static-route-group
Device(config-endpoint-tracker)# tracker-type tracker-group
Device(config-endpoint-tracker)# tracker-elements tcp-10001 udp-10002
Device(config-endpoint-tracker)# boolean and
Device(config-endpoint-tracker)# exit
Device(config)# track static-route-group endpoint-tracker
```

The following example shows how to configure tracker type as interface for a NAT DIA tracker endpoint:

```
Device(config)# endpoint-tracker tracker1
Device(config-endpoint-tracker)# tracker-type interface
Device(config-endpoint-tracker)# endpoint-dns-name www.cisco.com
Device(config-endpoint-tracker)# exit
```

The following example shows how to configure tracker type as tracker-group for a NAT DIA interface:

```
Device(config)# endpoint-tracker tracker1
Device(config-endpoint-tracker)# tracker-type interface
Device(config-endpoint-tracker)# endpoint-ip 10.1.1.1
Device(config-endpoint-tracker)# exit
Device(config)# endpoint-tracker tracker2
Device(config-endpoint-tracker)# tracker-type interface
Device(config-endpoint-tracker)# endpoint-dns-name www.cisco.com
Device(config-endpoint-tracker)# threshold 1000
Device(config-endpoint-tracker)# multiplier 10
Device(config-endpoint-tracker)# exit

Device(config)# endpoint-tracker group1
Device(config-endpoint-tracker)# tracker-type tracker-group
Device(config-endpoint-tracker)# tracker-elements tracker1 tracker2
Device(config-endpoint-tracker)# boolean or
Device(config-endpoint-tracker)# exit
```

The following example shows how to configure an ICMP tracker type for a NAT DIA interface:

```
Device(config)# endpoint-tracker tracker3
Device(config-endpoint-tracker)# tracker-type interface-icmp
Device(config-endpoint-tracker)# endpoint-ip 10.1.1.1
Device(config-endpoint-tracker)# threshold 100
Device(config-endpoint-tracker)# multiplier 5
Device(config-endpoint-tracker)# icmp-interval 2
```

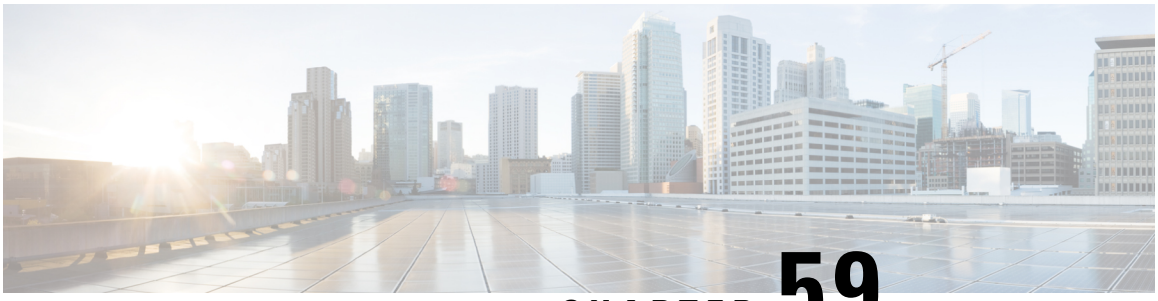
The following example shows how to configure an IPv6 ICMP tracker type for a NAT DIA interface:

```
Device(config)# endpoint-tracker tracker3
Device(config-endpoint-tracker)# tracker-type ipv6-interface-icmp
Device(config-endpoint-tracker)# ipv6-endpoint 2001:A1:F::5
Device(config-endpoint-tracker)# threshold 100
Device(config-endpoint-tracker)# multiplier 5
Device(config-endpoint-tracker)# icmp-interval 2
```

The following is a sample output from the **show endpoint-tracker** command for an IPv6 ICMP endpoint tracker applied to an interface.

```
Device# show endpoint-tracker

Interface                    Record Name            Status          Address Family    RTT
in msecs    Probe ID        Next Hop
GigabitEthernet1                  t2                 Up              IPv6              1
             6              2001:DB8:1::1
```



CHAPTER 59

Transport Gateway

- site-type, on page 867

site-type

Use the **site-type** command in system configuration mode to configure the site type of a router. Use the **no** form of the command to remove the site type assignment.

site-type *site-list*

no site-type *site-list*

Syntax Description

site-type *site-list*	Assigns up to four site types to a device. Possible values are br, branch, cloud, spoke, type-1, type-2, and type-3.

Command Default

By default, a router has no site type.

Command Modes

System (config-system)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	This command was introduced.

Example

The following example configures a router site type as cloud:

```
Device(config)#system
Device (config-system)# site-type cloud
```

The following example configures a router with site types cloud and branch:

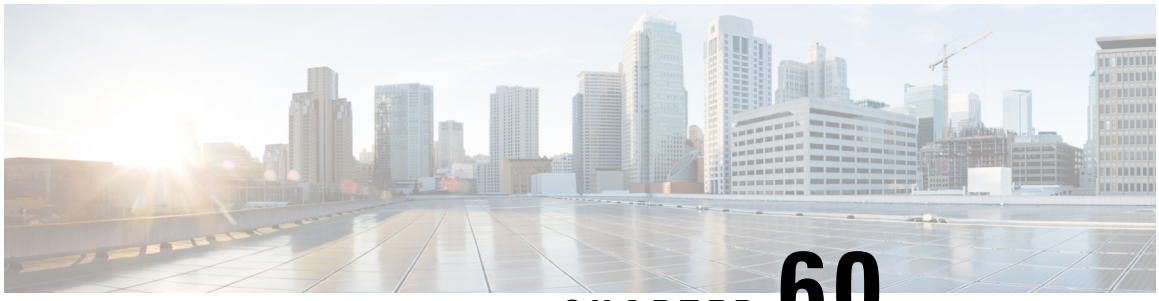
```
Device(config)#system
Device (config-system)# site-type cloud branch
```

The following example configures a router with site types cloud and branch, then removes the site type cloud, so that in the end, the router is configured only with site type branch:

```
Device(config)#system
Device (config-system)# site-type cloud branch
Device(config-system)# no site-type cloud
```

Related Commands

Command	Description
omp best-path transport-gateway	Use the **omp best-path transport-gateway** command to configure the path preference for transport gateway paths.



CHAPTER 60

UTD Commands

- file-analysis profile, on page 869
- file-inspection profile, on page 871
- file-reputation profile, on page 872
- flow-logging, on page 873
- logging host, on page 874
- threat-inspection profile, on page 874
- threat-inspection custom-signature profile, on page 875
- tls-decryption profile, on page 876
- utd engine standard multi-tenancy, on page 876
- utd engine standard unified-policy, on page 877
- utd global, on page 878
- utd multi-tenancy, on page 880
- web-filter url profile, on page 881

file-analysis profile

To configure Cisco Advanced Malware Protection (Cisco AMP) file analysis profile, use the **file-analysis profile** command in UTD Multi-Tenancy configuration mode. To delete Cisco AMP file analysis profile, use the **no** form of this command.

file-analysis profile *file-analysis-name* { **alert level** { **critical** | **info** | **warning** } | **file-types** *file-type* }
no file-analysis profile *file-analysis-name* { **alert level** { **critical** | **info** | **warning** } | **file-types** *file-type* }

Table 60: Syntax Description:

file-analysis-name	Specifies the file analysis profile name.
alert level critical |info |warning	Configures alert level as critical, info, or warning.

file-types *file-type*	Configures file types. Possible options are: • flv • mdb • mscab • msole2 • new-office • pdf • rtf • swf • wri • xlw

Command Default

None

Command Modes

UTD Multi-Tenancy configuration (config-utd-multi-tenancy).

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

File analysis is the process of submitting an unknown file to Cisco Secure Malware Analytics (formerly Threat Grid) cloud for Cisco IOS XE Catalyst SD-WAN Release 17.2.1v detonation in a sandbox environment. During detonation, the sandbox captures artefacts and observes behaviors of the file, then gives the file an overall score. Based on the observations and score, Threat Grid may change the threat response to Clean or Malicious. Findings from Threat Grid are reported back to the Cisco AMP cloud, so that all Cisco AMP customers are protected against newly discovered malware.

Examples

The following example shows how to configure an AMP file analysis profile with critical alerts, and a profile that analyzes flv and pdf files:

```
Device(config)# utd engine standard multi-tenancy
Device(config-utd-multi-tenancy)# file-analysis profile file-analysis-profile1
Device(config-utd-mt-file-an-profile)# alert level critical
Device(config-utd-mt-file-an-profile)# file-types
Device(config-utd-mt-file-an-types)# flv
Device(config-utd-mt-file-an-types)# pdf
```

Table 61: Related Commands

Commands	Description
utd multi-tenancy	Enables Unified Threat Defense (UTD) for multi-tenancy.
utd engine standard multi-tenancy	Configures UTD policies, web filtering, threat-inspection and Cisco AMP profiles for multi-tenancy (multiple tenants/VRFs).
file-inspection profile	Configures a file inspection profile.

file-inspection profile

To configure Cisco Advanced Malware Protection (Cisco AMP) file inspection profile, use the **file-inspection profile** command in UTD Multi-Tenancy configuration mode. To delete Cisco AMP file inspection profile, use the **no** form of this command.

file-inspection profile *file-inspection-profile* { **analysis profile** *file-analysis-name* | **reputation profile** *file-reputation-name* }
no file-inspection profile *file-inspection-profile* { **analysis profile** *file-analysis-name* | **reputation profile** *file-reputation-name* }

Table 62: Syntax Description:

file-inspection-profile	Specifies file inspection profile name.
file-analysis-name	Specifies file analysis profile name.
file-reputation-name	Specifies file reputation profile name.

Command Default

None

Command Modes

UTD Multi-Tenancy configuration (config-utd-multi-tenancy).

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Use the **file-inspection profile** command to configure an Cisco Advanced Malware Protection (Cisco AMP) file inspection profile.

Under the file inspection profile, a file reputation profile is required, and a file analysis profile is optional. Both must be configured first before assigning them to the file inspection profile.

Examples

The following example shows how to configure a file inspection profile that calls a file analysis and file reputation profiles:

```
Device(config)# utd engine standard multi-tenancy
Device(config-utd-multi-tenancy)# file-inspection profile file-inspection-profile1
Device(config-utd-mt-file-insp)# analysis profile file-analysis-profile1
Device(config-utd-mt-file-insp)# reputation profile file-reputation-profile1
```

After you configure the file-inspection profile, you can call it per VRF:

```
Device(config)# utd engine standard multi-tenancy
Device(config-utd-multi-tenancy)# policy utd-policy-vrf-1
Device(config-utd-mt-policy)# file-inspection profile file-inspection-profile1
Device(config-utd-mt-policy)# vrf 1
```

Table 63: Related Commands

Commands	Description
utd multi-tenancy	Enables Unified Threat Defense (UTD) for multi-tenancy.
utd engine standard multi-tenancy	Configures UTD policies, web filtering, threat-inspection and Cisco Advanced Malware Protection (Cisco AMP) profiles for multi-tenancy (multiple tenants/VRFs).
file-analysis profile	Configures a file analysis profile.
file-reputation profile	Configures a file reputation profile.
policy	Configures a policy under UTD and applies it to a VRF.

file-reputation profile

To configure Cisco Advanced Malware Protection (Cisco AMP) file reputation profile, use the **file-reputation profile** command in UTD Multi-Tenancy configuration mode. To delete a Cisco AMP file reputation profile, use the **no** form of this command.

file-reputation profile *file-reputation-name* [**alert level** { **critical** | **info** | **warning** }]
no file-reputation profile *file-reputation-name* [**alert level** { **critical** | **info** | **warning** }]

Syntax Description

file-reputation-name	Specifies file reputation profile name.
alert level critical | info | warning	Configures alert level as critical, info, or warning.

Command Default

None

Command Modes UTD Multi-Tenancy configuration (config-utd-multi-tenancy).

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines Use the **file-reputation profile** command to configure Cisco AMP file reputation profile, including the alert levels. We recommend configuring alert level info only when used for troubleshooting and not for regular traffic.

Examples

The following example shows how to configure Cisco AMP file reputation with critical alerts:

```
Device(config)# utd engine standard multi-tenancy
Device(config-utd-multi-tenancy)# file-reputation profile file-reputation-profile1
Device(config-utd-mt-file-rep-profile)# alert level critical
```

Table 64: Related Commands

Commands	Description
utdmulti-tenancy	Enables Unified Threat Defense (UTD) for multi-tenancy.
utdenginestandardmulti-tenancy	Configures UTD policies, web filtering, threat-inspection and Cisco Advanced Malware Protection (AMP) profiles for multi-tenancy (multiple tenants/VRFs).
file-inspectionprofile	Configures a file inspection profile.

flow-logging

To enable unified logging for UTD features use the **flow-logging** command in UTD Multi-Tenancy and unified-policy global configuration mode. To disable unified logging, use the **no** form of this command.

flow-logging [**all** | **file-inspection** | **threat-inspection** | **tls-decryption** | **web-filter**]

Command Default None

Command Modes UTD Multi-Tenancy and unified-policy global configuration (config-utd-mt-global)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Examples

The following example shows how to configure UTD logging in a unified security policy:

```
Device(config)# utd engine standard unified-policy
Device(config-utd-unified-policy)# utd global
Device(config-utd-mt-global)# flow-logging all
```

logging host

To log UTD syslog messages to a remote host, use the **logging host** command in UTD Multi-Tenancy and unified-policy global configuration mode. To remove a specified logging host from the configuration, use the **no** form of this command.

logging host *host_name* [**source-interface** *interface-name*]

Syntax Description

host-name	Host name or IP address of the host that will receive the UTD syslog messages. The character limit for logging servers is 114 to configure multiple FQDN UTD server.
interface-name	The interface from which the UTD syslog originates.

Command Default

None

Command Modes

UTD Multi-Tenancy and unified-policy global configuration (config-utd-mt-global)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Examples

The following example shows how to configure UTD logging in a unified security policy:

```
Device(config)# utd engine standard unified-policy
Device(config-utd-unified-policy)# utd global
Device(config-utd-mt-global)# logging host 10.1.1.1
Device(config-utd-mt-global)# logging host 10.2.2.2 source-interface GigabitEthernet3
```

threat-inspection profile

To configure threat-inspection profile and optionally specify the name of a custom signature profile, use the **threat-inspection profile** command in UTD unified policy configuration mode. To delete threat-inspection profile, use the **no** form of this command.

threat-inspection profile *threat-inspection-profile-name* **{custom-signature profile** *custom-signature-profile-name* **}**

no threat-inspection profile

Syntax Description

threat-inspection-profile-name	Specifies the threat-inspection profile name.
custom-signature profile *custom-signature-profile-name*	(Optional) Specifies the custom signature profile name.

Command Default

This command is not configured, and the IPS/IDS (Intrusion Prevention System and Intrusion Detection System) feature is not applied to traffic.

Command Modes

UTD unified policy configuration (config-utd-unified-policy)

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	Added support for specifying a custom-signature profile name.

Examples

The following example shows how to configure a threat-inspection profile:

```
Device(config)# utd engine standard unified-policy
Device(config-utd-unified-policy)# threat-inspection profile IPS_UNIFIED_1
Device(config-utd-mt-threat)# custom-signature profile global
```

threat-inspection custom-signature profile

To add a custom signature profile to a threat-inspection profile, use the **threat inspection custom-signature profile** command in UTD unified policy configuration mode. To delete the custom signature file, use the **no** form of this command.

threat-inspection custom-signature profile *custom-signature-profile-name* **file** *path-to-custom-signature-file*
no threat-inspection custom-signature profile

Syntax Description

custom-signature profile name	Specifies the custom-signature profile name.
file *path to custom signature file*	Specifies the path to the custom-signature file.

Command Default

Custom signature profile is not added to threat inspection profile.

Command Modes

UTD unified policy configuration (config-utd-unified-policy)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	This command was introduced.

Usage Guidelines If the custom signature profile does not exist in the designated path, an empty file is created on that path.

Examples The following example shows how to add a custom signature profile to a signature package:

```
utd engine standard unified-policy
  threat-inspection custom-signature profile global
    file bootflash:GLOBAL_CUSTOM_SIG.txt
  threat-inspection profile IPS_UNIFIED_1
     threat protection
     policy security
     custom-signature profile global
```

tls-decryption profile

To configure tls-decryption profile, use the **tls-decryption profile** command in UTD unified policy configuration mode. To delete tls-decryption profile, use the **no** form of this command.

tls-decryption profile *tls-decryption profile name*
no tls-decryption profile

tls-decryption profile name	Specifies tls-decryption profile name.

Command Default None

Command Modes UTD unified policy configuration (config-utd-unified-policy).

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Examples

The following example shows how to configure a tls-decryption profile:

```
Device(config)# utd engine standard unified-policy
Device(config-utd-unified-policy)# tls-decryption profile tls
```

utd engine standard multi-tenancy

To configure UTD policies, web filtering, threat-inspection, and Cisco Advanced Malware Protection (Cisco AMP) profiles for multi-tenancy (multiple tenants/VRFs), use the **utd engine standard multi-tenancy** command in global configuration mode. To remove them, use the **no** form of this command.

utd engine standard multi-tenancy

Syntax Description

(none)	You enter a sub-mode UTD engine standard multi-tenancy and configure UTD policies, web filtering, threat-inspection, and Advanced Malware Protection (AMP) profiles. After exiting the UTD engine standard multi-tenancy sub-mode, the UTD policies are applied.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Use the **utd engine standard multi-tenancy** command to configure UTD policies, web filtering, threat-inspection, and Cisco Advanced Malware Protection (Cisco AMP) profiles for multi-tenancy (multiple tenants/VRFs).

Before you begin, remove any existing single-tenancy UTD configuration, using the **no utd engine standard** command, and you must have previously configured a VRF for each tenant. Once you have done that, you can start configuring the policies that should be enforced for each tenant.

Examples

The following example shows how to configure UTD policies, web filtering, threat-inspection, and Cisco AMP profiles for multi-tenancy (multiple tenants/VRFs):

```
Device(config)# utd multi-tenancy
Device(config)# utd engine standard multi-tenancy
```

Table 65: Related Commands

Command	Description
utd multi-tenancy	Enables UTD policies for multi-tenancy (multiple tenants/VRFs).

utd engine standard unified-policy

To configure a unified security policy that includes firewall and other UTD profiles such as web filtering, threat-inspection, and Cisco Advanced Malware Protection (Cisco AMP), TLS decryption, use the **utd engine standard unified-policy** command in global configuration mode. To remove them, use the **no** form of this command.

utd engine standard unified-policy

Syntax Description

(none)	Enter a sub-mode UTD engine standard unified-policy and configure a unified security policy. After exiting the UTD engine standard unified-policy sub-mode, the unified security policies are applied.

Command Default None

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines Use the **utd engine standard unified-policy** command to configure unified security policy, web filtering, threat-inspection, Cisco Advanced Malware Protection (Cisco AMP) profiles, and TLS decryption.

Examples

The following example shows how to configure a unified policy with web filtering, threat-inspection, Cisco AMP profiles, and TLS decryption.

```
Device(config)# utd engine standard unified-policy
Device(config-utd-unified-policy)# policy aip-policy
Device(config-utd-mt-policy)# threat-inspection profile ips
Device(config-utd-mt-policy)# web-filter url profile url
Device(config-utd-mt-policy)# file-inspection profile fs
Device(config-utd-mt-policy)# tls-decryption profile tls
```

utd global

To configure settings that apply to all configured Unified Threat Defense (UTD) policies, use the **utd global** command in UTD Multi-Tenancy configuration mode. To remove the setting, use the **no** form of this command.

utd global { **file-analysis** [**apikey 0** *string*] | **cloud-server** *string* | **file-reputation** { **cloud-server** *string* | **est-server** *string* | **query-interval** *time* | **flow-logging** | **ip** | **logging** | **threat-inspection** | **web-filter** } }
no utd global { **file-analysis** [**apikey 0** *string*] | **cloud-server** *string* | **file-reputation** { **cloud-server** *string* | **est-server** *string* | **query-interval** *time* | **flow-logging** | **ip** | **logging** | **threat-inspection** | **web-filter** } }

Table 66: Syntax Description

(none)	Applies UTD policies to all tenants/VRFs. Multiple settings can be configured once the command is applied.
file-analysis	Configures Cisco AMP Threat Grid File analysis settings.
apikey 0 *string*	Specifies Cisco AMP Threat Grid API Key.
cloud-server *string*	Specifies Cisco AMP Threat Grid file analysis server. Example: cloud-isr-asn.amp.cisco.com
file-reputation	Specifies Cisco AMP File reputation settings.

cloud-server *string*	Specifies Cisco AMP Cloud server. Example: cloud-isr-asn.amp.cisco.com
est-server *string*	Specifies Cisco AMP EST server. Example: cloud-isr-est.amp.cisco.com
query-interval *time*	Specifies the query interval in seconds.
flow-logging	Configures unified logging for UTD features.
ip name-server*primary-ip-addresssecondary-ip-address*	(Optional) Specifies the preferred primary and an optional secondary IPv4 DNS server for the name-servers, thereby overriding the default OpenDNS name-servers and the IOSd configured name-servers.
logging	Configures global logging and syslog host settings.
threat-inspection*threat-inspection-profile-name*	Specifies the threat-inspection profile name.
web-filter*web-filter-profile-id*	Specifies web filter url profile name.

Command Default

None

Command Modes

UTD Multi-Tenancy configuration (config-utd-multi-tenancy).

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

To configure settings that apply to all configured UTD policies, use the **utd global** command in UTD Multi-Tenancy configuration mode.

By default, the UTD engine relies on hardcoded OpenDNS servers and the device's system-configured name-servers for URL lookups. However, in regions where OpenDNS access is restricted or experiences high latency, you can explicitly override these defaults using the **ip name-server** CLI command. By using **ip name-server**, you can manually specify custom primary and secondary DNS servers for the UTD engine. This configuration ensures that URL filtering services remain fully operational and maintain optimal performance in regions where OpenDNS access is restricted or unavailable. For more information, see Configure URL Filtering.

Usage Guidelines

.

Examples

The following example shows how to configure global AMP settings:

```
Device(config)# utd engine standard multi-tenancy
Device(config-utd-multi-tenancy)# utd global
Device(config-utd-mt-global)# file-analysis
Device(config-utd-mt-file-an-global)# apikey 0 0123456789abcdef
Device(config-utd-mt-file-an-global)# cloud-server cloud-isr-asn.amp.cisco.com
```

```
Device(config-utd-mt-file-an-global)# file-reputation
Device(config-utd-mt-file-rep-global)# cloud-server cloud-isr-asn.amp.cisco.com
Device(config-utd-mt-file-rep-global)# est-server cloud-isr-est.amp.cisco.com
Device(config-utd-mt-file-rep-global)# query-interval 900
```

The following example how to use the ip name-server command within the utd global configuration to override default lookups:

```
Device(config)# utd engine standard unified-policy
Device(config-utd-multi-tenancy)# utd global
Device(config-utd-mt-url-global)# ip name-server 10.8.8.8 10.8.4.4
```

Table 67: Related Commands

Commands	Description
utd multi-tenancy	Enables UTD for multi-tenancy.
utd engine standard multi-tenancy	Configures UTD policies, web filtering, threat-inspection and Cisco AMP profiles for multi-tenancy (multiple tenants/VRFs).

utd multi-tenancy

To enable Unified Threat Defense (UTD) for multi-tenancy (multiple tenants/VRFs), use the **utd multi-tenancy** command in global configuration mode. To disable UTD for multi-tenancy, use the **no** form of this command.

utd multi-tenancy [**engine standard multi-tenancy**]

Syntax Description

(none)	Enables UTD for multi-tenancy (multiple tenants/VRFs).

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Use the **utd multi-tenancy** command to enable UTD multi-tenancy mode. Single-tenancy mode is the default.

Examples

The following example shows how to enable UTD for multi-tenancy (multiple tenants/VRFs):

```
Device(config)# utd multi-tenancy
```

Table 68: Related Commands

Command	Description
utd engine standard multi-tenancy	Configures UTD policies, web filtering, threat-inspection and Cisco Advanced Malware Protection (Cisco AMP) profiles for multi-tenancy (multiple tenants/VRFs).

web-filter url profile

To configure web-filter url profile, use the **web-filter url profile** command in UTD unified policy configuration mode. To delete web-filter url profile, use the **no** form of this command.

web-filter url profile *web-filter-profile-id*
no web-filter url profile

web-filter-profile-id	Specifies web filter url profile name.

Command Default

None

Command Modes

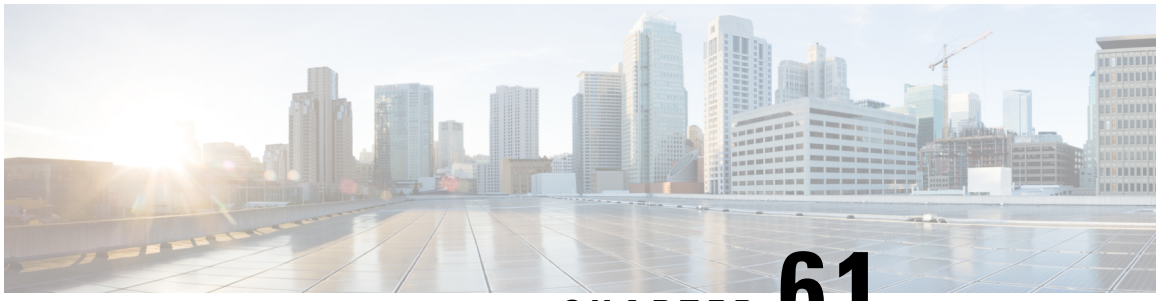
UTD unified policy configuration (config-utd-unified-policy).

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Examples

The following example shows how to configure a web filter url profile:

```
Device(config)# utd engine standard unified-policy
Device(config-utd-unified-policy)# web-filter url profile url
```



CHAPTER 61

VDSL Commands

- bitswap, on page 883
- controller VDSL, on page 884
- description (VDSL controller), on page 885
- diagnostics DELT (VDSL controller), on page 885
- firmware phy filename, on page 886
- line-mode bonding, on page 887
- line-mode single-wire line , on page 888
- modem (VDSL controller), on page 889
- operating mode, on page 889
- sra, on page 890
- sync interval, on page 891
- sync mode (VDSL controller), on page 892
- training log filename (VDSL controller), on page 893

bitswap

To divert the data of a disturbed transmission channel to other channels, use the **bitswap** command in controller configuration mode. To disable bitswapping, use the **no** form of this command.

bitswap
no bitswap

Command Default

Bit swapping is enabled.

Command Modes

Controller configuration (config-controller)#

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

bitswap line 0/1 commands are not supported in Cisco SD-WAN.

For usage guidelines, see the Cisco IOS XE `bitswap` command.

Examples

The following example shows how to enable bit swapping:

```
Router(config-controller)# bitswap
```

The following example shows how to disable bit swapping:

```
Router(config-controller)# no bitswap
```

controller VDSL

To configure the Very High Bit Rate Digital Subscriber Line (VDSL) controller and enter controller configuration mode, use the **controller VDSL** command in global configuration mode. This command does not have a **no** form.

controller VDSL *slot/subslot/port*

Syntax Description

slot	Slot number of the VDSL controller. Valid numbers are 0 and 1.
subslot	Subslot number of the VDSL controller. The slash mark (/) is required between the slot argument and the subslot argument.
port	Port number of the VDSL controller. Valid numbers are 0 and 1. The slash mark (/) is required between the subslot argument and the port argument.

Command Default

No default behavior or values.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Qualified for use in Cisco vManage CLI templates.

Usage Guidelines

This command is used to enter VDSL controller configuration mode for the controller in the specified slot, subslot, and port.

The **controller VDSL** command is supported only from global configuration mode. Configuring the command within the system configuration context may result in the following template deployment error:

```
bad value: "VDSL" is not a valid value.
```

Example

The following example shows how to enter VDSL controller configuration mode on the controller in slot 0, subslot 0, and port 0:

```
Device(config)# controller VDSL 0/0/0
```

description (VDSL controller)

To configure a text description for a VDSL controller, use the **description** command in VDSL controller configuration mode. To remove the text description for a VDSL controller, use the **no** form of this command.

description *string*
no description *string*

Syntax Description

string	VDSL controller text description.

Command Default

None

Command Modes

VDSL controller configuration (config-controller).

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

The Cisco multimode VDSL2 and ADSL1/2/2+ provides 1-port (2-pair) multimode VDSL2 and ADSL2+ WAN connectivity.

Use **description** command to configure a text description for a VDSL controller.

Example

The following example shows how to configure the description "to ISP 1" on the VDSL controller 0/0/0.

```
Device(config)# controller VDSL 0/0/0
Device(config-controller)# description to ISP 1
```

diagnostics DELT (VDSL controller)

To enable Double-Ended Line Testing (DELT) diagnostics mode for a VDSL controller, use the **diagnostics DELT** command in VDSL controller configuration mode. To disable the Double-Ended Line Testing (DELT) diagnostics mode for a VDSL controller, use the **no** form of this command.

diagnostics DELT
no diagnostics DELT

Syntax Description

This command has no keywords or arguments.

Command Default

By default, DELT diagnostics mode is disabled.

Command Modes

VDSL controller configuration (config-controller).

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

The Cisco multimode VDSL2 and ADSL1/2/2+ provides 1-port (2-pair) multimode VDSL2 and ADSL2+ WAN connectivity.

Double-Ended Line Testing (DELT) is a wideband line testing technique used after a DSL modem has been installed on the subscriber premises. It relies on the equipment on both ends of the line to perform its testing, thus requiring a connected and available DELT-capable CPE.

DELT measures the characteristics of the line by transmitting special test signals from one end to the other, and evaluating the signal received based on knowledge of the signal transmitted from the source.

Use **diagnosticsDELT** command to enable DELT diagnostics mode for a VDSL controller.

Example

The following example shows how to enable DELT diagnostics mode on the VDSL controller 0/0/0.

```
Device(config)# controller VDSL 0/0/0
Device(config-controller)# diagnostics DELT
```

firmware phy filename

To configure the Cisco IOS XE Catalyst SD-WAN device to load the VDSL controller firmware from a designated location, use the **firmware phy filename** command in VDSL controller configuration mode. To remove the configuration, use the **no** form of this command.

firmware phy filename *location:filename*
no firmware phy filename *location:filename*

Syntax Description

location:filename	Specifies the location and file name of VDSL firmware.

Command Default

None

Command Modes

VDSL controller configuration (config-controller).

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

VDSL2 and ADSL2/2+ routers provide highly reliable WAN connections for remote sites. These interfaces offer cost-effective virtualized WAN connections in both point-to-point and point-to-multipoint designs.

The Cisco multimode VDSL2 and ADSL1/2/2+ provides 1-port (2-pair) multimode VDSL2 and ADSL2+ WAN connectivity.

VDSL controllers have a firmware that can be upgraded separately from the IOS XE firmware. The VDSL controller firmware gets copied to a designated location on Cisco IOS XE Catalyst SD-WAN device. The Cisco IOS XE Catalyst SD-WAN device gets configured to load from the designated location and rebooted for the new firmware to take affect.

Use **firmware phy filename** command to configure the Cisco IOS XE Catalyst SD-WAN device to load the VDSL controller firmware from a designated location.

Example

The following example shows how to configure the Cisco IOS XE Catalyst SD-WAN device to load the VDSL controller firmware gs_39x3_gnu.pkg from bootflash.

```
Device(config)# controller VDSL 0/0/0
Device(config-controller)# firmware phy filename bootflash:gs_39x3_gnu.pkg
```

Table 69: Related Commands

Commands	Description
bitswap	Bit swap.
description	Controller specific description.
diagnostics	Diagnostics DELT.
line-mode	Line mode configuration to select Bonding/Single-wire.
modem	VDSL modem configuration.
operating	Configures auto or specific VDSL operating mode.
sra	Seamless rate adaptation.
sync	xDSL sync preferences.
training	DSL firmware training log.

line-mode bonding

To enable bonding mode on a CPE, use the **line-mode bonding** command in controller configuration mode. To disable the bonding mode, use the **no** form of this command.

line-mode bonding
no line-mode bonding

Syntax Description This command has no keywords or arguments.

Command Default Bonding is not the default mode.

Command Modes Controller configuration (config-controller)#

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

Use this command when a CPE is expected to operate in bonding mode. The command should be used only on DSL NIM-VAB-A. The configuration fails on other variants of NIM.

Examples

The following example shows how to enable bonding mode:

```
Router(config-controller)# line-mode bonding
```

The following example shows how to disable bonding mode:

```
Router(config-controller)# no line-mode bonding
```

line-mode single-wire line

To enable single-wire (nonbonding) mode on a selected line, use the **line-mode single-wire line** command in controller configuration mode. To disable the mode, use the **no** form of this command.

line-mode single-wire line *line-number*
or
line-mode single-wire line *line-number* **[profile 30a]**

no line-mode single-wire line *line-number*

Syntax Description

line-number	Line number. Valid values are either 1 or 0.
profile 30a	Enables 30a profile on line 1. If profile 30a is not specified, profiles 8a to 17a are enabled on that line.

Command Default

By default, single-wire mode is enabled on line 0 with profiles from 8a to17a enabled.

Command Modes

Controller configuration (config-controller)#

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

Use this command to configure either line 0 or line 1 in single-wire (non-bonding) mode. The command should be used only on DSL NIM-VAB-A. The configuration fails on other variants of NIM.

For usage guidelines, see the Cisco IOS XE line-mode single-wire line command.

Examples

The following example shows how to enable 30a profile on line 1:

```
Router(config-controller)# line-mode single-wire line 1 profile 30a
```

modem (VDSL controller)

To configure the modem settings for a VDSL controller, use the **modem** command in VDSL controller configuration mode. To remove the modem settings for a VDSL controller, use the **no** form of this command.

modem *modem-settings*
no modem *modem-settings*

Syntax Description

modem-settings	Specifies DSL modem settings.

Command Default

None

Command Modes

VDSL controller configuration (config-controller).

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

The Cisco multimode VDSL2 and ADSL1/2/2+ provides 1-port (2-pair) multimode VDSL2 and ADSL2+ WAN connectivity.

Modem setting commands allow custom configurations of DSL modem settings to ensure DSL interoperability in different environments. Please consult your Service Provider on required modem settings for the particular SPs network.

Use **modem** command to configure the modem settings for a VDSL controller.

Example

The following example shows how to configure the modem settings to enable the UK-specific Annex M mask on the VDSL controller 0/0/0.

```
Device(config)# controller VDSL 0/0/0
Device(config-controller)# modem customUKAnnexM
```

operating mode

To configure the operating mode for a VDSL controller, use the **operating mode** command in VDSL controller configuration mode. To remove the operating mode for a VDSL controller, use the **no** form of this command.

operating mode { **auto** [**adsl1**] [**adsl2**] [**adsl2+**] | **adsl1** | **adsl2** | **adsl2+** | **ansi** | **vdsl2** }
no operating mode { **auto** [**adsl1**] [**adsl2**] [**adsl2+**] | **adsl1** | **adsl2** | **adsl2+** | **ansi** | **vdsl2** }

Syntax Description

adsl1	Specifies the operating mode as adsl1 (ITU G 992.1).

adsl2	Specifies the operating mode as adsl2 (ITU G 992.3).
adsl2+	Specifies the operating mode as adsl2+ (ITU G 992.5).
ansi	Specifies the operating mode as adsl2/2+ mode, as defined in ITU G.991.1, G.992.3, and G992.5.
auto	Specifies the operating mode as auto.
vdsl2	Specifies the operating mode as vdsl2 (ITU G 993.2).

Command Default

The default operating mode is auto.

Command Modes

VDSL controller configuration (config-controller).

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates. The following command options are qualified: **auto**, **adsl1**, **adsl2**, **adsl2+**, **auto adsl1**, **auto adsl2**, **auto adsl2+**, **vdsl2**.

Usage Guidelines

The Cisco multimode VDSL2 and ADSL1/2/2+ provides 1-port (2-pair) multimode VDSL2 and ADSL2+ WAN connectivity.

You choose the operating mode depending on what DSL technology your ISP uses.

Use **operating mode** command to configure the operating mode for a VDSL controller.

Example

The following example shows how to configure the VDSL controller 0/0/0 operating mode to auto.

```
Device(config)# controller VDSL 0/0/0
Device(config-controller)# operating mode auto
```

sra

To accommodate changes to the total link capacity with the least amount of disruption to communications, use the **sra** command in controller configuration mode.

sra

Command Default

Seamless rate adaptation is disabled.

Command Modes

Controller configuration (config-controller)#

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

sra line 0/1 commands are not supported in Cisco SD-WAN.

For usage guidelines, see the Cisco IOS XE `sra line` command.

Examples

The following example shows how to enable seamless rate adaptation:

```
Router(config-controller)# sra
```

sync interval

To specify an interval for the device to exchange Precision Time Protocol synchronization messages, use the **sync interval** command in PTP port configuration mode. To disable a sync interval configuration, use the **no** form of this command.

sync interval *interval-value*
no sync interval *interval-value*

Syntax Description

interval-value	Value of the interval at which the device sends sync packets. The intervals are set using log base 2 values, as follows: • 4—1 packet every 16 seconds • 3—1 packet every 8 seconds • 2—1 packet every 4 seconds • 1—1 packet every 2 seconds • 0—1 packet every second • -1—1 packet every 1/2 second, or 2 packets per second • -2—1 packet every 1/4 second, or 4 packets per second • -3—1 packet every 1/8 second, or 8 packets per second • -4—1 packet every 1/16 seconds, or 16 packets per second • -5—1 packet every 1/32 seconds, or 32 packets per second • -6—1 packet every 1/64 seconds, or 64 packets per second The recommended value is -6.

Command Default

The default value is 1.

Command Modes

PTP port configuration (config-ptp-port)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Command qualified for use in Cisco vManage CLI templates.

Examples

The following example shows how to configure the PTP sync interval:

```
Device> enable
Device# configure terminal
Device(config)# ptp clock ordinary domain 0
Device(config-ptp-clk)# clock-port slave slaveport
Device(config-ptp-port)# sync interval -4
Device(config-ptp-port)# end
```

sync mode (VDSL controller)

To configure the synchronization mode preference for a VDSL controller, use the **sync mode** command in VDSL controller configuration mode. To remove the synchronization mode preference for a VDSL controller, use the **no** form of this command.

sync mode { **ansi** [**previous**] | **itu** [**previous**] | **none** }
no sync mode { **ansi** [**previous**] | **itu** [**previous**] | **none** }

Syntax Description

ansi	Sets the synchronization mode preference to ANSI over ITU.
itu	Sets the synchronization mode preference to ITU over ANSI.
none	Sets the synchronization mode to no preferred mode.
previous	(Optional) Informs the router to save the current trained mode and to try that mode during the next synchronization.

Command Default

None

Command Modes

VDSL controller configuration (config-controller).

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

The Cisco multimode VDSL2 and ADSL1/2/2+ provides 1-port (2-pair) multimode VDSL2 and ADSL2+ WAN connectivity.

The CPE tries to synchronize in ANSI and ITU modes and **sync mode** command specifies which mode should be tried first.

Use **sync mode** command to configure the synchronization mode preference for a VDSL controller.

Example

The following example shows how to configure the synchronization mode preference to ANSI on the VDSL controller 0/0/0.

```
Device(config)# controller VDSL 0/0/0
Device(config-controller)# sync mode ansi previous
```

training log filename (VDSL controller)

To modify the location and name of the file in which training logs are stored for a VDSL controller, use the **training log filename** command in VDSL controller configuration mode. To reset the location and name of the file in which training logs are stored for a VDSL controller back to the default, use the **no** form of this command.

training log filename *filename*
no training log filename *filename*

Syntax Description

filename	Specifies location and filename of training logs.

Command Default

None

Command Modes

VDSL controller configuration (config-controller).

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

The Cisco multimode VDSL2 and ADSL1/2/2+ provides 1-port (2-pair) multimode VDSL2 and ADSL2+ WAN connectivity.

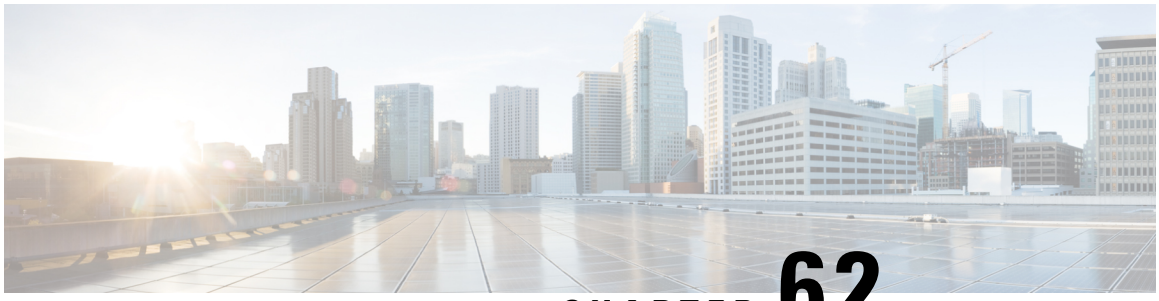
A training log provides you information about the different events that happened during the ADSL training.

Use **training log filename** command to modify the location and name of the file in which training logs are stored for a VDSL controller.

Example

The following example shows how to modify the location and filename on the VDSL controller 0/0/0 to bootflash:VDSLLOG.log.

```
Device(config)# controller VDSL 0/0/0
Device(config-controller)# training log filename bootflash:VDSLLOG.log
```



CHAPTER 62

Voice Commands

- allow-connections, on page 896
- bind interface, on page 897
- caller-id alerting dsp-pre-allocate, on page 897
- caller-id alerting line-reversal, on page 898
- caller-id alerting pre-ring, on page 899
- caller-id alerting ring, on page 900
- caller-id block, on page 901
- caller-id enable, on page 902
- caller-id format e911, on page 903
- caller-id mode, on page 903
- clid dtmf-codes, on page 905
- codec preference, on page 906
- credentials, on page 907
- description (dial-peer voice voip), on page 908
- destination-pattern, on page 908
- dial-peer voice (VOIP), on page 910
- dtmf-relay (VOIP), on page 910
- hunt-scheme least-used, on page 911
- hunt-scheme round-robin, on page 912
- hunt-scheme sequential, on page 913
- id network, on page 913
- keepalive retries, on page 914
- keepalive timeout, on page 915
- max-dn, on page 915
- max-pool, on page 916
- registrar server, on page 916
- security-policy (voice register global), on page 917
- session protocol, on page 918
- session-transport, on page 919
- sccp ip precedence, on page 920
- system message (voice register global), on page 920
- sip, on page 921
- sip-ua, on page 921

- supplementary-service sip, on page 922
- **translation-profile (voice register)**, on page 923
- voice-class codec (voice register pool), on page 924
- voice-class codec (dial peer voice), on page 925
- voice class codec, on page 925
- voice register global, on page 926
- voice register pool, on page 927
- voice service voip, on page 927

allow-connections

To allow connections between specific types of endpoints in a VoIP network, use the **allow-connections** command in voice service configuration mode (**voice service voip**). To refuse specific types of connections, use the **no** form of this command.

allow-connections sip to sip
no allow-connections sip to sip

Syntax Description

sip	Originating endpoint type, **sip** --Session Interface Protocol (SIP).
to	Indicates that the argument that follows is the connection target.
sip	Terminating endpoint type.

Command Default

SIP-to-SIP connections are disabled by default.

Command Modes

Voice-service configuration (config-voi-serv) using the **voice service voip** command

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `allow-connections` command.

Examples

```
voice service voip

  allow-connections sip to sip
  no supplementary-service sip handle-replaces
  no supplementary-service sip moved-temporarily
  no supplementary-service sip refer
  sip
   registrar server expires max 300 min 200
```

bind interface

To bind an interface to a Cisco CallManager group, use the **bindinterface** command in SCCP Cisco CallManager configuration mode. To unbind the selected interface, use the **no** form of this command.

Supported Parameters

interface-type	Type of the selected interface.
interface-number	Number of the selected interface.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE bind interface command. As per the yang model design, configure **sip-ua** command on device then under SIP command, configure **bind interface**.

Examples

```
bind interface <interface-name-slot/bay/port>
keepalive retries <1-32>
keepalive timeout <0-180>
sccp ip precedence <1-7>
```

caller-id alerting dsp-pre-allocate

To statically allocate a digital signal processor (DSP) resource for receiving caller ID information for an on-hook (Type 1) caller ID at a receiving Foreign Exchange Office (FXO) voice port, use the **caller-id alerting dsp-pre-allocate** command in voice-port configuration mode. To disable the effect of the command, delete the command from the CLI add-on feature template.

caller-id alerting dsp-pre-allocate

Syntax Description

alerting	Defines the caller ID alerting method.
dsp-pre-allocate	Performs DSP preallocation.

Command Default

DSP resource for receiving caller ID information are not allocated.

Command Modes

Voice-port configuration (config-voiceport)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	This command was introduced.

Usage Guidelines

Before using this command, enable caller ID with the **caller-id enable** command.

The **caller-id alerting dsp-pre-allocate** command may be required on an FXO port if the central office uses line polarity reversal to signal the start of caller ID information transmission. Preallocating a DSP voice channel allows the DSP voice channel to listen for caller ID information continuously without requiring an alerting signal from the central office.

Examples

The following example shows how to configure a voice port at which the caller ID information is to be received:

```
voice-port 1/0/0
  cptone br
  caller-id enable
  caller-id alerting line-reversal
  caller-id alerting dsp-pre-allocate
```

caller-id alerting line-reversal

To set the line-reversal alerting method for caller ID information for an on-hook (Type 1) caller ID at a sending Foreign Exchange Station (FXS) voice port, and for an on-hook caller ID at a receiving Foreign Exchange Office (FXO) voice port, use the **caller-id alerting line-reversal** command in voice-port configuration mode. To disable the effect of the command, delete the command from the CLI add-on feature template.

caller-id alerting line-reversal

Syntax Description

alerting	Defines the caller ID alerting method.
line-reversal	Enables line-reversal alerting.

Command Default

The line-reversal alerting method for caller ID information is not set.

Command Modes

Voice-port configuration (config-voiceport)

Command History

Release	Modification
Cisco SD-WAN Release 20.8.1	This command was introduced.

Usage Guidelines

Before using this command, enable caller ID with the **caller-id enable** command.

Before using this command, use the **caller-id mode** command to specify a noncountry, standard caller ID mode, or use the **cptone** command to specify a regional analog voice-interface-related tone, ring, and cadence setting for a voice port:

- **caller-id mode** {**BT** | **FSK** | **DTMF start** *x* **end** *y* }.

- **cptone** *locale*, Here, *locale* can be **FR**, **DE**, **NO** , **IT**, **ES**, **ZA**, **TR**, **GB**, **AT**, **CN**, **HU**, **KR**, **BR**, **SE**, **DK**, **IS**, **NL**, **BE**, **IN**, or **SA**.

Examples

The following example shows how to configure a voice port from which caller ID information is sent (FXS):

```
voice-port 1/0/0
   cptone br
   caller-id name A-sample
   caller-id number 4085550111
   caller-id enable
   caller-id alerting line-reversal
```

The following example shows how to configure a voice port from which caller ID information is received (FXO):

```
voice-port 2/0/0
   cptone br
   caller-id enable
   caller-id alerting line-reversal
   caller-id alerting dsp-pre-allocate
```

caller-id alerting pre-ring

To set a 250-millisecond pre-ring alerting method for caller ID information for an on-hook (Type 1) caller ID at a sending Foreign Exchange Station (FXS) and at a receiving Foreign Exchange Office (FXO) voice port, use the **caller-id alerting pre-ring** command in voice-port configuration mode. To disable the effect of the command, delete the command from the CLI add-on feature template.

caller-id alerting pre-ring

Syntax Description

alerting	Defines the caller ID alerting method.
pre-ring	Enables a 250-millisecond pre-ring alerting method for caller ID information.

Command Default

A 250-millisecond pre-ring alerting method for caller ID information is not set.

Command Modes

Voice-port configuration (config-voiceport)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	This command was introduced.

Usage Guidelines

This command is required only when the telephone device attached to an FXS port requires the pre-ring (immediate ring) method to signal the start of caller ID transmission. Use it on FXS voice ports that send caller ID information. This command allows the FXS port to send a short pre-ring before the normal ring

cadence. On an FXO port, an incoming pre-ring is simply counted as a normal ring by use of the **caller-id alerting ring** command.

Before using this command, enable caller ID with the **caller-id enable** command.

Before using this command, use the **caller-id mode** command to specify a noncountry, standard caller ID mode, or use the **cptone** command to specify a regional analog voice-interface-related tone, ring, and cadence setting for a voice port:

- **caller-id mode** {**BT** | **FSK** | **DTMF start** *x* **end** *y* }.
- **cptone** *locale*, Here, *locale* can be **FR**, **DE**, **NO** , **IT**, **ES**, **ZA**, **TR**, **GB**, **AT**, **CN**, **HU**, **KR**, **BR**, **SE**, **DK**, **IS**, **NL**, **BE**, **IN**, or **SA**.

Examples

The following example shows how to configure a voice port from which caller ID information is sent:

```
voice-port 1/0/0
   cptone br
   caller-id enable
   station name A-sample
   station number 4085550111
   caller-id alerting pre-ring
```

The following example shows how to configure a voice port from which caller ID information is received (FXO):

```
voice-port 2/0/0
   cptone br
   caller-id enable
   caller-id alerting pre-ring
```

caller-id alerting ring

To set the ring-cycle method for receiving caller ID information for an on-hook (Type 1) caller ID at a receiving Foreign Exchange Office (FXO) or a sending Foreign Exchange Station (FXS) voice port, use the **caller-id alerting ring** command in voice-port configuration mode. To disable the effect of the command, delete the command from the CLI add-on feature template.

caller-id alerting ring [**1** | **2** | **3** **4**]

Syntax Description

alerting	Defines the caller ID alerting method.
ring [1 | 2 | 3 | 4]	Sets number of ring ON cycles. The default value is 1.

Command Default

The ring-cycle method for receiving caller ID information is set to 1.

Command Modes

Voice-port configuration (config-voiceport)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	This command was introduced.

Usage Guidelines

Before using this command, enable caller ID with the **caller-id enable** command .

The caller ID alerting ring setting is determined by the Bellcore/Telcordia or ETSI standard that your telephone service provider uses for caller ID. Use the setting in the FXO loop-start and ground-start voice ports at which the caller ID information arrives, and in the FXS voice ports from which caller ID information is sent.

This setting must match on the sending and receiving ends of the telephone line connection.

Examples

The following example shows how to configure a voice port at which the caller ID information is received (FXO):

```
voice-port 2/0/0
   cptone US
   caller-id enable
   caller-id alerting ring 2
```

The following example shows how to configure a voice port from which caller ID information is sent (FXS):

```
voice-port 1/0/0
   cptone us
   station name A-sample
   station number 4085550111
   caller-id enable
   caller-id alerting ring 2
```

caller-id block

To request blocking of caller ID information display at the far end of a call that originates from a Foreign Exchange Station (FXS) port, use the **caller-id block** command in voice-port configuration mode at the originating FXS voice port. To allow the display of caller ID information, delete the command from the CLI add-on feature template.

caller-id block

Syntax Description

block	Blocks the caller ID of calls that are made from this port.

Command Default

The display of caller ID information is allowed.

Command Modes

Voice-port configuration (config-voiceport)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	This command was introduced.

Usage Guidelines

Before using this command, enable caller ID with the **caller-id enable** command.

Examples

The following example shows how to configure a voice port from which caller ID information is sent to block the display of caller ID information:

```
voice-port 1/0/0
   caller-id enable
   caller-id block
```

caller-id enable

To enable a device to accept configuration settings from a **caller-id** command that configures caller ID functionality, use the **caller-id enable** command in voice-port configuration mode at the originating FXS or the receiving FXO voice port. To prevent a device from accepting configuration settings from a **caller-id** command that configures caller ID functionality, delete this command from the CLI add-on feature template.

caller-id enable

Syntax Description

enable	Enables a device to accept configuration settings from a **caller-id** command.

Command Default

This command is not configured.

Command Modes

Voice-port configuration (config-voiceport)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	This command was introduced.

Usage Guidelines

Configure the **caller-id enable** command before using any of the following commands:

- **caller-id alerting dsp-pre-allocate**
- **caller-id alerting line-reversal**
- **caller-id alerting pre-ring**
- **caller-id alerting ring**
- **caller-id block**
- **caller-id format e911**
- **caller-id mode**

Examples

The following example shows how to enable a device to accept configuration settings from a **caller-id** command that configures caller ID functionality:

```
voice-port 1/0/0
   station name A-sample
   station number 4085550111
   caller-id enable
   caller-id alerting ring 2
```

caller-id format e911

To specify a caller ID message type that should be the Enhanced 911 format for calls sent on Foreign Exchange Station (FXS) voice ports, use the **caller-id format e911** command in voice-port configuration mode at the originating FXS voice port. To use the default Multiple Data Message Format (MDMF) caller ID message type, delete the command from the CLI add-on feature template.

caller-id format 911

Syntax Description

e911	Specifies the Enhanced 911 format.

Command Default

The MDMF caller ID message type is used.

Command Modes

Voice-port configuration (config-voiceport)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	This command was introduced.

Usage Guidelines

Before using this command, enable caller ID with the **caller-id enable** command.

Examples

The following example shows how to configure a voice port from which caller ID information is sent to use the Enhanced 911 format:

```
voice-port 1/0/0
   cptone US
   station name A-sample
   station number 4085550111
   caller-id enable
   caller-id format e911
```

caller-id mode

To specify a noncountry, standard caller ID mode, use the **caller-id mode** command in voice port configuration mode at the sending Foreign Exchange Station (FXS) voice port or at the receiving Foreign Exchange Office (FXO) voice port. To allow the caller ID mode to be country-specific, delete the command from the CLI add-on feature template.

caller-id mode { **BT** | **FSK** | **DTMF** [**start** | { **#** | ***** | **A** | **B** | **C** | **D** } | **end** | { **#** | ***** | **A** | **B** | **C** | **D** }] }

Syntax Description

BT	Specifies Frequency-Shift Keying (FSK) with Dual Tone Alerting Signal (DTAS) that is used by British Telecom.
FSK	Specifies that FSK be used before or during a call.
DTMF	Specifies that dual tone multifrequency (DTMF) digits be used with the start and end digit codes.
start	Specifies the start digit code for DTMF digits.
end	Specifies the end digit code for DTMF digits.
#	Specifies the DTMF digit #.
*****	Specifies the DTMF digit *.
A	Specifies the DTMF digit A.
B	Specifies the DTMF digit B.
C	Specifies the DTMF digit C.
D	Specifies the DTMF digit D.

Command Default

The caller-ID mode is disabled.

Command Modes

Voice-port configuration (config-voiceport)

Command History

Release	Modification
Cisco SD-WAN Release 20.8.1	This command was introduced.

Usage Guidelines

Before using this command, enable caller ID with the **caller-id enable** command.

This command allows you to configure a caller ID mode that is different from the caller ID mode that the **cptone** *locale* command configuration command specifies.

The **caller-id mode DTMF** command allows you to configure caller ID DTMF start and end codes that are different from the caller ID DTMF start and end codes that the global **clid dtmf-codes** configuration specifies.

Examples

The following example shows how to configures a noncountry, standard caller ID mode of DTMF with a start code A and end code C:

```
voice-port 1/0/0
   station name A-sample
   station number 4085550111
   caller-id enable
   caller-id mode DTMF start A end C
```

clid dtmf-codes

To specify global caller ID dual-tone multifrequency (DTMF) start, redirect, and end codes, use the **clid dtmf-codes** command in voice service pots configuration mode. To disable the effect of the command, delete the command from the CLI add-on feature template.

clid dtmf-codes *start-code redirect-code end-code*

Syntax Description

dtmf-codes	Defines the DTMF codes.
start-code	Global start code for the DTMF caller ID string. Valid characters are: • Capital letters **A** through **D** • Numbers **0** through **9** • Asterisk (*****) • Pound sign (**#**)
redirect-code	Global redirect code for the DTMF caller ID string. Valid characters are: • Capital letters **A** through **D** • Numbers **0** through **9** • Asterisk (*****) • Pound sign (**#**)
end-code	Global end code for the DTMF caller ID string. Valid characters are: • Capital letters **A** through **D** • Numbers **0** through **9** • Asterisk (*****) • Pound sign (**#**)

Command Default

The methods for global caller ID DTMF start, redirect, and end codes are not set.

Command Modes

voice service pots configuration (conf-voi-serv)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	This command was introduced.

Usage Guidelines

This command is used to configure the global caller ID DTMF codes that are used if the **caller-id mode DTMF** command in voice-port *x*/*y*/*z* configuration mode is not configured.

Examples

The following example shows how to configure global caller ID DTMF start, redirect, and end codes to be A, B, and C, respectively:

```
voice service pots
      clid dtmf-codes ABC
```

codec preference

To specify a list of preferred codecs to use on a dial peer, use the **codec preference** command in voice class configuration mode. To disable this functionality, use the **no** form of this command.

codec preference *value* [*codec-type* [**bytes** *payload-size* | **mode** *mode-value*]]
no codec preference

Syntax Description

value	Order of preference. 1 is the most preferred and 24 is the least preferred.
codec-type	Preferred codec. Values are as follows: • **g711alaw** --G.711 a-law 64,000 bps. • **g711ulaw** --G.711 mu-law 64,000 bps. • **g722-64** --G.722-64 at 64,000 bps. • **g729r8** --G.729 8000 bps. • **ilbc** --internet Low Bitrate Codec (iLBC) at 13,330 bps or 15,200 bps. If this option is not specified, the dial peer uses the default codec for all calls.
bytes *payload-size*	(Optional) Specifies that the size (bytes) of the voice payload of each frame. Values depend on the codec type and the packet voice protocol. Applicable to: • **g711alaw** • **g711ulaw** • **g722-64** • **g729r8**
mode *mode-value*	(Optional, applies only to the internet low bitrate codec (iLBC), specified with the **ilbc** option.) Specifies bitrate. The following are valid values: • 20: Configures 15.2 kbps • 30: Configures 13.33 kbps The default value is 20.

Command Default If this command is not entered, no specific types of codecs are identified with preference.

Command Modes voice class configuration (config-class)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines For usage guidelines, see the Cisco IOS XE `codec preference` command.

Examples

```
voice class codec 1000
  codec preference 1 g729r8
  codec preference 2 g711ulaw bytes 160
  codec preference 3 g711alaw bytes 160
  codec preference 4 g722-64 bytes 160
```

credentials

To enter credentials configuration mode to configure a certificate for a Cisco Unified Communications Manager Express Certificate Ttrust List (CTL) provider or for Cisco Unified Survivable Remote Site Telephony (SRST) router communication to Cisco Unified Communications Manager, use the **credentials** command in global configuration mode. To set all the commands that are present in credentials configuration mode to the default **nonsecure**, use the **no** form of this command.

credentials
no credentials

Syntax Description This command has no arguments or keywords.

Command Default Nonsecure, so credentials are not provided.

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	This command was introduced.

Usage Guidelines The credential server provides certificates to any device that requests a certificate. The credentials server does not request any data from a client, and so, no authentication is necessary. When the client, Cisco Unified Communications Manager, requests a certificate, the credentials server provides the certificate. Cisco Unified Communications Manager exports the certificate to the phone, and the Cisco Unified IP phone holds the SRST router certificate in its configuration file. The device certificate for secure SRST routers is placed in the configuration file of the Cisco Unified IP phone because the entry limit in the CTL of Cisco Unified Communications Manager is 32.

Credentials service for SRST runs on default port 2445. Cisco Unified Communications Manager connects to port 2445 on the secure SRST router and retrieves the secure SRST device certificate during the TLS handshake.

Activate this command on all SRST routers.

Caution: For security reasons, credentials service should be deactivated on all the SRST routers after the task of provisioning to Cisco Unified Communications Manager is completed.

Examples

The following example shows how to enter credentials configuration mode and set the IP source address and the trustpoint:

```
credentials
  ip source-address 10.6.21.4 port 2445
  trustpoint srstca
```

description (dial-peer voice voip)

To add a description consisting of a line of up to 64 characters to describe a dial peer, use the **description** command in dial peer configuration mode. To delete the description, use the **no** form of this command.

description *string*
no description

Syntax Description

string	Description of dial peer, up to 64 characters.

Command Modes

Dial peer configuration (config-dial-peer)

Usage Guidelines

Use this command to include descriptive text about the dial peer. The description appears in **show** command output and does not affect the operation of the dial peer.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `description` command.

```
dial-peer voice 2000 voip
  description inbound PSTN calls
```

destination-pattern

To specify either the prefix or the full E.164 telephone number to be used for a dial peer, use the **destination-pattern** command in dial peer configuration mode.

destination-pattern *string*

no destination-pattern *string*

Syntax Description

string	Series of digits that specify a pattern for the E.164 or private dialing plan telephone number. Valid entries are the digits 0 through 9, the letters A through D, and the following special characters: • The asterisk (*) and pound sign (#) that appear on standard touch-tone dial pads. • Comma (,), which inserts a pause between digits. • Period (.), which matches any entered digit (this character is used as a wildcard). • Percent sign (%), which indicates that the preceding digit occurred zero or more times; similar to the wildcard usage. • Circumflex (^), which indicates a match to the beginning of the string. • Dollar sign ($), which matches the null string at the end of the input string. • Backslash symbol (\), which is followed by a single character, and matches that character. Can be used with a single character with no other significance (matching that character). • Question mark (?), which indicates that the preceding digit occurred zero or one time. • Brackets ([ ]), which indicate a range. A range is a sequence of characters enclosed in the brackets; only numeric characters from 0 to 9 are allowed in the range. • Parentheses (( )), which indicate a pattern and are the same as the regular expression rule.

Command Modes

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

Use the **destination-pattern** command to define the E.164 telephone number for a dial peer.

The pattern you configure is used to match dialed digits to a dial peer. The dial peer is then used to complete the call. When a router receives voice data, it compares the called number (the full E.164 telephone number) in the packet header with the number configured as the destination pattern for the voice-telephony peer. The router then strips out the left-justified numbers that correspond to the destination pattern. If you have configured a prefix, the prefix is prepended to the remaining numbers, creating a dial string that the router then dials. If all numbers in the destination pattern are stripped out, the user receives a dial tone.

For usage guidelines, see the Cisco IOS XE `destination-pattern` command.

```
dial-peer voice 1000 voip
  description         Branch 1

  destination-pattern 1T
  no shutdown
  voice-class codec 1000
  session transport udp
  session protocol sipv2
  session target ipv4:10.1.101.8
  dtmf-relay rtp-nte digit-drop sip-kpml sip-notify
```

dial-peer voice (VOIP)

To define a particular dial peer, to specify the method of voice encapsulation, and to enter dial peer configuration mode, use the **dial-peer voice** command in global configuration mode. To delete a defined dial peer, use the **no** form of this command.

dial-peer voice *dial-peer-tag* **voip**
no dial-peer voice

dial-peer-tag	Dial peer tag.

Command Default

No dial peer is defined. No method of voice encapsulation is specified.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

Use the **dial-peer voice** global configuration command to switch to dial peer configuration mode from global configuration mode and to define a particular dial peer. Use the **exit**command to exit dial peer configuration mode and return to global configuration mode.

For usage guidelines, see the Cisco IOS XE `dial-peer voice` command.

```
dial-peer voice 1000 voip
  description         Branch 1

  destination-pattern 1T
  no shutdown
  voice-class codec 1000
  session transport udp
  session protocol sipv2
  session target ipv4:10.1.101.8
  dtmf-relay rtp-nte digit-drop sip-kpml sip-notify
```

dtmf-relay (VOIP)

To specify how a Session Initiation Protocol (SIP) gateway relays dual tone multifrequency (DTMF) tones between telephony interfaces and an IP network, use the **dtmf-relay**command in dial peer voice configuration mode. To remove all signaling options and send the DTMF tones as part of the audio stream, use the **no** form of this command.

dtmf-relay { **rtp-nte** [**digit-drop** | **sip-info** | **sip-kpml** | **sip-notify**] | **sip-info** [**rtp-nte** [**digit-drop**] | **sip-kpml** | **sip-notify**] | **sip-kpml** [**rtp-nte** [**digit-drop**] | **sip-info** | **sip-notify**] | **sip-notify** [**rtp-nte** [**digit-drop**] | **sip-info** | **sip-kpml**] }

no dtmf-relay { **rtp-nte** | **sip-info** | **sip-kpml** | **sip-notify** }

Syntax Description

rtp-nte	Forwards DTMF tones by using RTP with the Named Telephone Event (NTE) payload type.
digit-drop	Passes digits out-of-band and drops in-band digits. **Note** The **digit-drop**keyword is only available when the **rtp-nte** keyword is configured.
sip-info	Forwards DTMF tones using SIP INFO messages. This keyword is available only if the VoIP dial peer is configured for SIP.
sip-kpml	Forwards DTMF tones using SIP KPML over SIP SUBSCRIBE/NOTIFY messages. This keyword is available only if the VoIP dial peer is configured for SIP.
sip-notify	Forwards DTMF tones using SIP NOTIFY messages. This keyword is available only if the VoIP dial peer is configured for SIP.

Command Default

DTMF tones are disabled and sent in-band. That is, they are left in the audio stream.

Command Modes

Dial peer voice configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `dtmf-relay (Voice over IP)` command.

```
dial-peer voice 1000 voip
  description Branch 1

  destination-pattern 1T
  no shutdown
  voice-class codec 1000
  session transport udp
  session protocol sipv2
  session target ipv4:10.1.101.8
  dtmf-relay rtp-nte digit-drop sip-kpml sip-notify
```

hunt-scheme least-used

To enable the least used search method for finding an available channel in a trunk group for outgoing calls, use the **hunt-scheme least-used** command in trunk group configuration mode. To delete the hunt scheme from the trunk group profile, use the **no** form of the command.

Supported Parameters

both	Searches both even- and odd-numbered channels.

even	Searches for an idle even-numbered channel. If no idle even-numbered channels are available, an odd-numbered channel is sought.
odd	Searches for an idle odd-numbered channel. If no idle odd-numbered channels are available, an even-numbered channel is sought.
up	Searches channels in ascending order based within a trunk group member. Used with **even**, **odd**, **both**.
down	Searches channels in descending order within a trunk group member. Used with **even**, **odd**, **both**.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE hunt-scheme least-used command.

hunt-scheme round-robin

To enable the round robin search method for finding an available channel in a trunk group for outgoing calls, use the **hunt-scheme round-robin** command in trunk group configuration mode. To delete the hunt scheme from the trunk group profile, use the **no** form of this command.

Supported Parameters

both	Searches for an idle channel among both even- and odd-numbered channels at the same precedence.
even	Searches for an idle even-numbered channel. If no idle even-numbered channel is available, an odd-numbered channel is used.
odd	Searches for an idle odd-numbered channel. If no idle odd-numbered channel is available, an even-numbered channel is used.
up	Searches channels in ascending order based within a trunk group member. Used with **even**, **odd**, **both**.
down	Searches channels in descending order within a trunk group member. Used with **even**, **odd**, **both**.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE hunt-scheme round-robin command.

hunt-scheme sequential

To specify the sequential search method for finding an available channel in a trunk group for outgoing calls, use the **hunt-scheme sequential** command in trunk group configuration mode. To delete the hunt scheme from the trunk group profile, use the **no** form of this command.

Supported Parameters

both	Searches both even- and odd-numbered channels.
even	Searches for an idle even-numbered channel. If no idle even-numbered channel is available, an odd-numbered channel is sought.
odd	Searches for an idle odd-numbered channel. If no idle odd-numbered channel is available, an even-numbered channel is sought.
up	Searches channels in ascending order based within a trunk group member. Used with **even**, **odd**, **both**.
down	Searches channels in descending order within a trunk group member. Used with **even**, **odd**, **both**.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE hunt-scheme sequential command.

Examples

```
hunt-scheme sequential [both | even | odd] [up | down]
```

id network

To configure the IPv4 prefixes of the network that contains IP phones that Survivable Remote Site Telephony (SRST) supports, use the **id network** command in voice register pool configuration mode. To remove the prefixes, use the no form of this command.

id network *address* **mask** *mask*

Syntax Description

address	Specifies the IPv4 prefix.
mask	Specifies the IP subnet mask.

Command Default

This command has no default behavior.

Command Modes Voice register pool configuration (config-register-pool)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines The command can be used to configure the IPv4 prefixes of the network that contains the IP phones that SRST supports.

Example

The following example show how to configure 10.10.10.0/24 as the network that contains the IP phones that the SRST feature supports.

```
Device(config)# voice register pool 100
Device(config-register-pool)# id network 10.10.10.0 mask 255.255.255.0
```

Related Commands

Command	Description
voice register pool	Enters voice register pool configuration mode.

keepalive retries

To set the number of keepalive retries from Skinny Client Control Protocol (SCCP) to Cisco Unified CallManager, use the **keepalive retries** command in SCCP Cisco CallManager configuration mode. To reset this number to the default value, use the **no** form of this command.

Supported Parameters

number	Number of keepalive attempts. Range is 1 to 32. Default is 3.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines For more information about this command, see the Cisco IOS XE keepalive retries command.

Examples

```
bind interface <interface-name-slot/bay/port>
keepalive retries <1-32>
sccp ip precedence <1-7>
```

keepalive timeout

To set the length of time between keepalive messages from Skinny Client Control Protocol (SCCP) to Cisco Unified CallManager, use the **keepalive timeout** command in SCCP Cisco CallManager configuration mode. To reset the length of time to the default value, use the **no** form of this command.

Supported Parameters

seconds	Time between keepalive messages. Range is 1 to 180. Default is 30.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE keepalive timeout command.

Examples

```
bind interface <interface-name-slot/bay/port>
keepalive timeout <0-180>
sccp ip precedence <1-7>
```

max-dn

To set the maximum number of extensions to be supported by a Cisco Unified SIP SRST router, use the **max-dn** command in voice register global mode (**voice register global**). To reset this number to the default value, use the **no**form of this command.

max-dn *max-directory-numbers*

no max-dn

Syntax Description

max-directory-numbers	Maximum number of phone directory numbers to allow in the Cisco Unified SIP SRST system. The maximum you can set depends on the software version, router platform, and amount of memory that you have installed. Type **?** to display range. The default is 0.

Command Default

The default is 0.

Command Modes

Voice register global

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

The **max-dn** command limits the number of directory numbers available in a Cisco Unified SIP SRST system. The maximum number of ephone-dns that you can create depends on the software version, router platform, and amount of memory that you have installed. Type **?** to display range.

```
voice register global
 max-dn   200
 max-pool 100
 system message "SRST mode"
```

max-pool

To set the maximum number of Session Initiation Protocol (SIP) voice register pools that are supported in Cisco Unified SIP SRST, use the **max-pool** command in voice register global configuration mode (**voice register global**). To reset the maximum number to the default, use the **no** form of this command.

max-pool *max-voice-registers-pools*

no max-pool

Syntax Description

max-voice-registers-pools	Maximum number of SIP voice register pools supported by the Cisco router. The upper limit of voice register pools is platform-dependent; type **?** for range.

Command Modes

Voice register global configuration (config-register-global)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

This command limits the number of SIP phones supported by Cisco Unified SIP SRST. The **max-pool** command is platform specific and defines the limit for the **voice register pool** command.

The **max-dn** command similarly limits the number of directory numbers (extensions) in Cisco Unified SIP SRST.

```
voice register global
  max-dn   200
  max-pool 100
  system message "SRST mode"
```

registrar server

To enable SIP registrar functionality, use the **registrar server** command in SIP configuration mode (**voice service voip**, then **sip**). To disable SIP registrar functionality, use the **no**form of the command.

registrar server expires [**max** *sec* [**min** *sec*] | **min** *sec*]

no registrar server

Syntax Description

expires	(Optional) Sets the active time for an incoming registration.
max*sec*	(Optional) Maximum expires time for a registration, in seconds. The range is from 600 to 86400. The default is 3600.
min*sec*	(Optional) Minimum expires time for a registration, in seconds. The range is from 60 to 3600. The default is 60.

Command Default

SIP registrar functionality on the Cisco Unified SRST router is disabled.

Command Modes

SIP configuration (conf-serv-sip)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

This command enables SIP phone registrations to SIP SRST during fallback mode. If this command is not entered, then phones will not register to SRST.

```
voice service voip

  allow-connections sip to sip
  no supplementary-service sip handle-replaces
  no supplementary-service sip moved-temporarily
  no supplementary-service sip refer
  sip
   registrar server expires max 300 min 200
```

security-policy (voice register global)

To define the security level of Session Initiation Protocol (SIP) phones allowed to register, use the **security-policy command** command in voice register global configuration mode. To return to the default, use the **no** form of this command.

security-policy secure
no security-policy secure

Syntax Description

secure	Requires SIP phones to use Transport Layer Security (TLS) for signaling transport. Non\-secure SIP phones are blocked from registering. This functionality is valid for Cisco Unified Survivable Remote Site Telephony (SRST).

Command Default

Phones of all security levels are permitted to register, which also is referred to as device-default mode.

Command Modes

Voice register global configuration (config-register-global)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	This command was introduced.

Usage Guidelines

The **secure** keyword configures the SIP registration security policy so that only encrypted phones can register to the Cisco Unified SRST device in the event of a failover from the primary call control. When this keyword is configured, nonsecure phones that use TCP or UDP for signaling transport, and authenticated phones that use TLS/TCP for signaling transport are blocked from registering.

Examples

The following example shows that only registration requests from encrypted SIP phones in a Cisco Unified SRST system are permitted:

```
voice register global
  security-policy secure
```

session protocol

To configure the session protocol for dial peer, use the **session protocol** command in dial-peer group configuration mode. To remove the session protocol configuration, use the **no** form of this command.

session protocol sipv2 [**target** *target*]

Syntax Description

target *target*	Specifies the IP address of the target to forward voice calls. Example: **ipv4:10.1.101.8**

Command Default

Session Initiation Protocol (SIP) version 2 is the only supported protocol for voice dial peer with Cisco SD-WAN.

Command Modes

Dial-peer group configuration (config-dial-peer)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

The command can be used to configure SIP v2 as the session protocol. In addition, you can configure an IPv4 address as target to route the call towards for outbound VOIP dial-peers.

Example

The following examples show how to configure SIPv2 as the session protocol for a voice dial-peer, and configure the IP 10.1.101.8 as target to route the call to for outbound VOIP dial-peers.

```
Device(config)# dial-peer voice 1000 voip
Device(config-dial-peer)# session protocol sipv2 target ipv4:10.1.101.8
```

```
Device(config)#  dial-peer voice 1000 voip
Device(config-dial-peer)# session protocol sipv2
Device(config-dial-peer)# session target ipv4:10.1.101.8
```

Related Commands

Command	Description
dial-peer voice	Enter dial-peer group configuration mode.

session-transport

To specify the transport layer protocol that a SIP phone uses to connect to Cisco Unified SIP gateway, use the **session-transport** command in voice service voip sip or dial-peer voice modes. To reset to the default value, use the **no** form of this command.

session-transport { **tcp** [**tls**] | **udp** }

no session-transport

Syntax Description

tcp	Transmission Control Protocol (TCP) is used.
tls	(Available only with the **tcp** option) Transport layer security (TLS) over TCP.
udp	User Datagram Protocol (UDP) is used. This is the default.

Command Default

UDP is the default protocol.

Command Modes

voice service voip sip

dial-peer voice

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

This command sets the transport layer protocol parameter in the phone's configuration file.

```
dial-peer voice 8000 voip
  description         Branch 7
   destination-pattern 8T
  no shutdown
  voice-class codec 1000
  session transport udp
  session protocol sipv2
  session target ipv4:10.1.101.8
  dtmf-relay rtp-nte digit-drop sip-kpml sip-notify
```

sccp ip precedence

To set the IP precedence value to be used by Skinny Client Control Protocol (SCCP), use the **sccp ip precedence** command in global configuration mode. To reset to the default, use the **no** form of this command.

Supported Parameters

value	IP precedence value. Range is from 1 (lowest) to 7 (highest).

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE sccp ip precedence command.

Examples

```
bind interface <interface-name-slot/bay/port>
keepalive retries <1-32>
keepalive timeout <0-180>
sccp ip precedence <1-7>
```

system message (voice register global)

To define a message that displays on SIP phones in a Cisco Unified Survivable Remote Site Telephony (Cisco Unified SRST) system, use the **system message** command in voice register global configuration mode (accessible using the **voice register global** command). To return to the default, use the **no** form of this command.

system message *string*
no system message

Syntax Description

string	Message that displays on SIP phones after the phones failover to Cisco Unified SRST. The string can contain a maximum of 32 alphanumeric characters.

Command Default

There is no default message.

Command Modes

Voice register global configuration (config-register-global)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

The command allows you to customize the idle prompt message that displays on the status line of SIP phones after the phones lose connection with Cisco Unified Communications Manager and failover to Cisco Unified

SRST. A configured message displays until the phones fallback to Cisco Unified Communications Manager. There is no default message.

```
voice register global
  max-dn   200
  max-pool 100
  system message "SRST mode"
```

sip

To enter the Session Initiation Protocol (SIP) configuration mode, use the **sip** command in voice-service VoIP configuration mode.

sip

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Voice-service VoIP configuration (config-voi-srv)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

From the voice-service VoIPconfiguration mode, the **sip** command enables you to enter SIP configuration mode.

For usage guidelines, see the Cisco IOS XE `sip` command.

```
voice service voip

  allow-connections sip to sip
  no supplementary-service sip handle-replaces
  no supplementary-service sip moved-temporarily
  no supplementary-service sip refer
  sip
   registrar server expires max 300 min 200
```

sip-ua

To enable Session Initiation Protocol (SIP) user-agent configuration commands, use the **sip-ua** command in global configuration mode. To reset all SIP user-agent configuration commands to their default values, use the **no** form of this command.

sip-ua
no sip-ua

Syntax Description This command has no arguments or keywords.

Command Default If this command is not enabled, no SIP user-agent configuration commands can be entered.

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines For usage guidelines, see the Cisco IOS XE `sip-ua` command.

Examples The following example shows how to enter SIP user-agent configuration mode and configure the SIP user agent:

```
Device> enable
Device# configure terminal
Device(config)# sip-ua
```

supplementary-service sip

To enable SIP supplementary service capabilities for call forwarding and call transfers across a SIP network, use the **supplementary-service sip** command in voice service VOIP configuration mode (**voice service voip**). To disable supplementary service capabilities, use the **no** form of this command.

supplementary-service sip { **handle-replaces** [**moved-temporarily**] [**refer**] | **moved-temporarily** [**handle-replaces**] [**refer**] | **refer** [**handle-replaces**] [**moved-temporarily**] }
no supplementary-service sip { **handle-replaces** | **moved-temporarily** | **refer** }

Syntax Description

handle-replaces	Replaces the Dialog-ID in the Replaces Header with the peer Dialog-ID.
moved-temporarily	Enables SIP Redirect response for call forwarding.
refer	Enables SIP REFER message for call transfers.

Command Default SIP supplementary service capabilities are enabled globally.

Command Modes Voice service configuration (conf-voi-serv)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines For usage guidelines, see the Cisco IOS XE `supplementary-service sip` command.

```
voice service voip

 allow-connections sip to sip
 no supplementary-service sip handle-replaces
 no supplementary-service sip moved-temporarily
 no supplementary-service sip refer
 sip
  registrar server expires max 300 min 200
```

translation-profile (voice register)

To apply a translation profile to incoming or outgoing call legs on a SIP phone in a Cisco Unified Survivable Remote Site Telephony (SRST) system, use the **translation-profile** command in voice register dn or voice register pool configuration mode. To remove the translation profile, use the **no** form of this command.

translation-profile { **incoming** | **outgoing** } *name*
no translation-profile { **incoming** | **outgoing** }

Syntax Description

incoming	Specifies that this translation profile handles incoming calls.
outgoing	Specifies that this translation profile handles outgoing calls.
name	Name of the translation profile.

Command Default

Translation profile is not assigned to call legs on the phone.

Command Modes

Voice register dn configuration (config-register-dn)

Voice register pool configuration (config-register-pool)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	This command was introduced.

Usage Guidelines

This command assigns a predefined translation profile to incoming or outgoing call legs to and from the Cisco Unified SRST router. Use this command to apply the translation profile to a specific directory number or to all directory numbers on a SIP phone. Create the translation profile that you want to assign is created by using the **voice translation-profile** command.

Examples

The following example assigns the translation profile named profile1 to handle translation of outgoing calls from SIP phone 21:

```
voice register pool 21
  translation-profile outgoing profile1
```

The following example assigns the translation profile named profile2 to handle translation of incoming calls to extension 1200:

```
voice register dn 12
  number 1200
  translation-profile incoming profile2
```

voice-class codec (voice register pool)

To assign a previously configured codec selection preference list, use the **voice-class codec** command in voice register pool configuration mode. To remove the codec preference assignment from the voice register pool, use the **no** form of this command.

voice-class codec *tag*

no voice-class codec

Syntax Description

tag	Unique number assigned to the voice class. Range is from 1 to 10000. The tag number maps to the tag number created by using the **voice-class codec** command in dial-peer configuration mode.

Command Default

There is no codec preference assignment in the voice register pool configuration.

Command Modes

Voice register pool configuration mode

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

During Cisco Unified Session Initiation Protocol (SIP) Survivable Remote Site Telephony (SRST) registration, a dial peer is created and that dial peer includes codec g729r8 by default. This command allows you to change the automatically selected default codec.

The **id** (voice register pool) command is required and must be configured before any other voice register pool commands. The **id** command identifies a locally available individual Cisco SIP IP phone or set of Cisco SIP IP phones.

```
dial-peer voice 8000 voip
  description Branch 7
   destination-pattern 8T
  no shutdown
  voice-class codec 1000
  session transport udp
  session protocol sipv2
  session target ipv4:10.1.101.8
  dtmf-relay rtp-nte digit-drop sip-kpml sip-notify
```

voice-class codec (dial peer voice)

To assign a previously configured codec selection preference list (codec voice class) to a voice over IP (VoIP) dial peer, use the **voice-class codec** command in dial-peer configuration mode. To remove the codec preference assignment from the dial peer, use the **no** form of this command.

voice-class codec *tag*

no voice-class codec

Syntax Description

tag	Unique number assigned to the voice class. Range: 1 to 10000. The tag number maps to the tag number created using the **voice class codec** global configuration command.

Command Default

Dial peers have no codec voice class assigned.

Command Modes

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

You can assign one voice class to each VoIP dial peer. If you assign another voice class to a dial peer, the last voice class assigned replaces the previous voice class.

```
dial-peer voice 100 voip
  voice-class codec 10
```

voice class codec

To enter voice-class configuration mode and assign an identification tag number for a codec voice class, use the **voice class codec** command in global configuration mode. To delete a codec voice class, use the **no** form of this command.

voice class codec *tag value*

Syntax Description

tag	Lets you specify the unique number that you assign to the voice class. Range is from 1 to 10000. There is no default.
value	Specifies the order of preference. 1 is the most preferred and 24 is the least preferred value.

Command Default

This command has no default behavior.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

This command only creates the voice class for codec selection preference and assigns an identification tag. Use the **codec preference** command inside the codec class mode to specify the preference of the voice codec.

Example

The following example show how to configure voice class for codec selection preference and assigns 1 as identification tag.

```
Device(config)# voice class codec 1
Device(config-class)# codec preference 1 g729r8
Device(config-class)# codec preference 2 g711alaw
```

voice register global

To enter voice register global configuration mode in order to set global parameters for all supported Cisco SIP IP phones in a Cisco Unified Session Initiation Protocol (SIP) Survivable Remote Site Telephony (SRST) environment, use the **voice register global** command in global configuration mode. To automatically remove the existing DNs, pools, and global dialplan patterns, use the **no**form of this command.

voice register global

no voice register global

Syntax Description

This command has no arguments or keywords.

Command Default

There are no system-level parameters configured for SIP IP phones.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Cisco Unified SIP SRST

Use this command and configure max-pool and max-dn to all SIP phone registrations to SRST.

```
voice register global
  max-dn   200
  max-pool 100
  system message "SRST mode"
```

voice register pool

To enter voice register pool configuration mode and create a pool configuration for a set of SIP phones in Cisco Unified SIP SRST, use the **voice register pool** command in global configuration mode. To remove the pool configuration, use the **no** form of this command.

voice register pool *pool-tag*

no voice register pool *pool-tag*

Syntax Description

pool-tag	Unique number assigned to the pool.

Command Default

There is no pool configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Cisco Unified SIP SRST

Use this command to enable user control on which registrations are to be accepted or rejected by a SIP SRST device. The voice register pool command mode can be used for specialized functions and to restrict registrations on the basis of the IP subnet parameter.

```
voice register global
  max-dn   200
  max-pool 100
  system message "SRST mode"
 voice register pool 100
  id network 10.0.0.0 mask 255.0.0.0
```

voice service voip

To configure voice-service VoIP, use the **voice service voip** command in global configuration mode. To remove the VoIP voice service, use the **no** form of this command.

voice service voip

Command Default

This command has no default behavior.

Command Modes

This command has no default behavior.

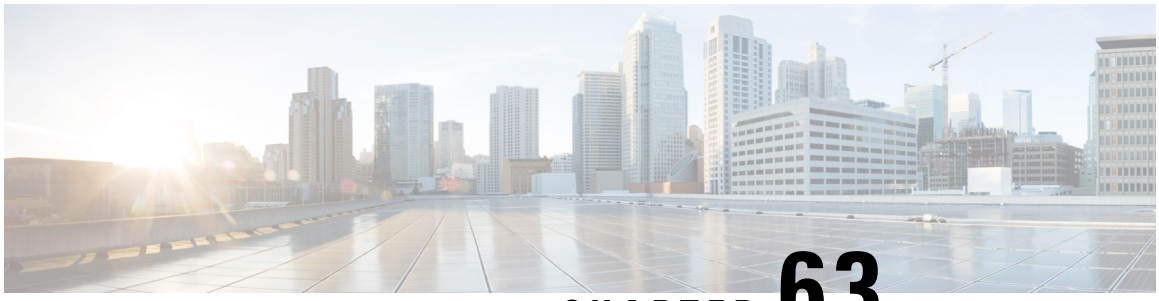
Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Example

The following example show how to configure voice-service VoIP.

```
Device(config)# voice service voip
```



CHAPTER 63

VRF Commands

- address-family ipv4, on page 929
- address-family ipv6, on page 931
- description (VRF definition), on page 932
- ip vrf, on page 932
- platform ipreass boost-mode, on page 933
- rd (VPLS), on page 933
- redistribute vrf, on page 934
- route-replicate (VRF address family), on page 937
- route-target, on page 938
- service tcp-keepalives-in, on page 939
- service tcp-keepalives-out, on page 940
- service tcp-small-servers, on page 940
- service udp-small-servers, on page 941
- vrf definition, on page 941

address-family ipv4

To set an address family ipv4 in vrf configuration mode use the **address-family ipv4** command. To remove the IPv4 address-family, use the **no** form of this command.

address-family ipv4 { **bgp** [*next-hop*] | **export** [*map*] | **import** [*map*] | **maximum** [*routes*] | **mdt** [*auto-discovery* | *data* | *default* | *log-reuse* | *mtu* | *overlay* | *preference*] | **route-replicate** [*from* | *recursion-policy*] | **route-target** [*export* | *import*] }
no address-family ipv4 { **bgp** [*next-hop*] | **export** [*map*] | **import** [*map*] | **maximum** [*routes*] | **mdt** [*auto-discovery* | *data* | *default* | *log-reuse* | *mtu* | *overlay* | *preference*] | **route-replicate** [*from* | *recursion-policy*] | **route-target** [*export* | *import*] }

Syntax Description

bgp	A standardized exterior gateway protocol designed to exchange routing and reachability information.
next-hop	IP address of the next hop in the traffic flow.
export	Allows vrf table to be exported to the global table or another vrf.
map	VRF definition or global table.

import	Allows global table or another vrf table to be imported to vrf.
map	VRF definition or global table.
maximum	Specifies the max number of routes.
routes	<0 – 42949677295>
mdt	Specifies an IPv4 multicast distribution tree (MDT) address family session.
auto-discovery	Enables BGP MVPN discovery for GRE in multicast code.
data	Specifies a range of addresses to be used in the data multicast distribution tree (MDT) pool.
default	Configures a default multicast distribution tree (MDT) group for a vrf.
log-reuse	Enables the recording of data multicast distribution tree (MDT) reuse.
mtu	Defines the largest size of packets that an interface can transmit.
overlay	Specifies a protocol as the overlay.
preference	Specifies a preference for a particular MDT type (MLDP or PIM).
route-replicate	Replicates routes into the base topology within the specified address family.
from	Defines a vrf where network resides.
recursion-policy	
route-target	Specifies the target where routes are ether sent or received.
export	Allows a vrf table to be exported to the global table or another vrf.
import	Allows a global table or another vrf table to be imported to vrf.

Command Default

None

Command Modes

VRF configuration (config-vrf)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

The **address-family ipv4** command under the vrf definition allows you to configure routing sessions and other related configuration commands.

Example

The following example shows the how to configure **address-family ipv4** prefixes from vrf 77.

```
Device(config)# vrf definition 77
Device(config-vrf)# address-family ipv4
Device(config-ipv4)# exit-address-family
```

address-family ipv6

To set an address family ipv6 in vrf configuration mode use the **address-family ipv6** command. To remove the IPv6 address-family, use the **no** form of this command.

address-family ipv6 { **bgp** [*next-hop*] | **import** [*map*] | **mdt** [*auto-discovery* | *data* | *default* | *log-reuse* | *mtu* | *overlay* | *preference*] }
no address-family ipv6 { **bgp** [*next-hop*] | **import** [*map*] | **mdt** [*auto-discovery* | *data* | *default* | *log-reuse* | *mtu* | *overlay* | *preference*] }

Syntax Description

bgp	A standardized exterior gateway protocol designed to exchange routing and reachability information.
next-hop	IP address of the next hop in the traffic flow.
import	Allows global table or another vrf table to be imported to vrf.
map	VRF definition or global table.
mdt	Specifies an IPv6 multicast distribution tree (MDT) address family session.
auto-discovery	Enables BGP MVPN discovery for GRE in multicast code.
data	Specifies a range of addresses to be used in the data multicast distribution tree (MDT) pool.
default	Configures a default multicast distribution tree (MDT) group for a vrf.
log-reuse	Enables the recording of data multicast distribution tree (MDT) reuse.
mtu	Defines the largest size of packets that an interface can transmit.
overlay	Specifies a protocol as the overlay.
preference	Specifies a preference for a particular MDT type (MLDP or PIM).

Command Default

None

Command Modes

VRF configuration (config-vrf)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

The **address-family ipv6** command under the vrf definition allows you to configure routing sessions and other related configuration commands.

Example

The following example shows the how to configure **address-family ipv6** prefixes from vrf 77.

```
Device(config)# vrf definition 77
Device(config-vrf)# address-family ipv6
Device(config-ipv6)# exit-address-family
```

description (VRF definition)

To assign a helpful description to a virtual routing and forwarding (VRF) instance, use the **description** command in VRF definition configuration mode. To remove the description, use the **no** form of this command.

description *string*
no description

Syntax Description

string	Description of a VRF (up to 244 characters).

Command Default

This command has no default arguments or keywords.

Command Modes

VRF definition configuration mode (config-vrf)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For the usage guideline, see description (VRF definition)

Examples

```
Device(config)# vrf definition 1
Device(config-vrf)# description vrf instance 1
```

ip vrf

To define a VPN routing and forwarding (VRF) instance and to enter VRF configuration mode, use the **ip vrf** command in global configuration mode. To remove a VRF instance, use the **no** form of this command.

Supported Parameters

vrf-name	Name assigned to a VRF.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE ip vrf command.

Examples

The following example shows how to import a route map to a VRF instance named VPN1:

```
Router(config)# ip vrf vpn1
Router(config-vrf)# rd 100:2
Router(config-vrf)# route-target both 100:2
Router(config-vrf)# route-target import 100:1
```

platform ipreass boost-mode

To enable boost mode for IP reassembly, use the **platform ipreass boost-mode** command in global configuration mode. To disable IP reassembly boost mode, use the **no** form of this command.

platform ipreass boost-mode
no platform ipreass boost-mode

Syntax Description

boost-mode	Boosts the hardware-accelerated IPSec packet processing and throughput capabilities.

Command Default

IP reassembly boost mode is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	The command was introduced.

Usage Guidelines

Configure the **platform ipreass boost-mode** command during a maintenance window.

The CLI displays the following warning for the boost-mode keyword:

```
Warning: please configure this command during maintenance window
```

The **platform ipreass boost-mode** command can be entered without any additional keywords. The **threshold** keyword is available as an optional completion after platform ipreass boost-mode.

To determine whether tunnel underlay reassembly boost mode is active use the command **show platform hardware qfp active infrastructure cvla client handles**. For more information, refer to Verify VFR and underlay fragments.

Examples

```
Device(config)# platform ipreass boost-mode
```

rd (VPLS)

To specify a route distinguisher (RD) to distribute endpoint information in a Virtual Private LAN Service (VPLS) configuration, use the **rd** command in L2 VFI configuration or VFI autodiscovery configuration

mode. To remove the manually configured RD and return to the automatically generated RD, use the **no** form of this command.

rd {*autonomous-system-number*:*nn* | *ip-address*:*nn*}
no rd {*autonomous-system-number*:*nn* | *ip-address*:*nn*}

Syntax Description

autonomous-system-number:*nn*	Specifies a 16-bit autonomous system number (ASN) and 32-bit arbitrary number. The ASN does not have to match the local autonomous system number.
ip-address:*nn*	Specifies a 32-bit IP address and a 16-bit arbitrary number. Only IPv4 addresses are supported.

Command Default

VPLS autodiscovery automatically generates a RD using the Border Gateway Protocol (BGP) autonomous system number and the configured virtual forwarding instance (VFI) VPN ID.

Command Modes

VRF definition configuration mode (config-vrf)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For the usage guideline, see rd (VPLS)

Examples

```
Device(config)# vrf definition 1
Device(config-vrf)# rd 1:2
```

redistribute vrf

To redistribute routes that are replicated between global VRF and service VPN and between inter-service VPNs, use the **redistribute vrf** command in router configuration mode. To stop such redistribution, use the **no** form of this command.

redistribute vrf *vrf-name protocol* [**metric** *bandwidth-metric delay-metric reliability-metric effective-bandwidth-metric mtu-bytes*] **subnets** [**route-map** *route-map-name*]
no redistribute vrf *vrf-name protocol* **subnets** [**metric** *bandwidth-metric delay-metric reliability-metric effective-bandwidth-metric mtu-bytes*] [**route-map** *route-map-name*]

Syntax Description

vrf-name	The name of the VRF from which routes are replicated.

protocol	Type of protocol of the source route. Some of the keywords require an argument. The valid keywords and arguments are: • **bgp** *autonomous-system-number* : Border Gateway Protocol (BGP). • **connected** : Connected routes. • **eigrp** *autonomous-system-number* : Enhanced Interior Gateway Routing Protocol (EIGRP). • **ospf** *process-id* : Open Shortest Path First (OSPF). • **static** : Static routes. • **nhrp** : Next Hop Resolution Protocol (NHRP) routes.
route-map-name	(Optional) Name of a route map that filters out routes that shouldn't be redistributed back to the original protocol.
metric	(Optional) Specifies the metric for redistributed routes.
bandwidth-metric	(Optional) Maximum bandwidth of the route in kilobits per second (kb/s). The range is 1 to 4294967295.
delay-metric	(Optional) EIGRP route delay metric in microseconds. The range is 1 to 4294967295.
reliability-metric	(Optional) EIGRP reliability metric. The range is 0 to 255. An EIGRP metric of 255 signifies 100 percent reliability.
effective-bandwidth-metric	(Optional) Effective bandwidth of the route. The range is 1 to 255. The effective bandwidth of 255 denotes 100 percent load.
mtu-bytes	(Optional) Smallest allowed value for the maximum transmission unit (MTU) in bytes. The range is 1 to 65535.
subnets	(Optional) Specifies redistribution of routes into OSPF. When routes are redistributed into OSPF, only routes that are not subnetted are redistributed if the **subnets** keyword is not specified. This is not applicable for connected protocol type. This can be configured for bgp, nhrp, ospf, ospfv3, and static protocol types. By default, no subnets are defined.

Command Default

No routes are redistributed.

Command Modes

Router topology configuration (config-router-af-topology)

Router configuration (config-router)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Support is added for BGP as the destination protocol when redistributing between the global VRF and service VPNs.
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	Support is added for redistrbuting between service VRFs on the same edge device site.

Examples

The following example shows how to redistribute global VRF routes into VRF EIGRP that were replicated from global BGP to service VPN:

```
Device(config)# vrf definition 1
Device(config-vrf)# address-family ipv4
Device(config-ipv4)# route-replicate from vrf global unicast bgp 56
Device(config-ipv4)# exit-address-family
Device(config-vrf)# exit
Device(config)# router eigrp test
Device(config-router)# ! Redistribute routes that were replicated from vrf global into
eigrp.
Device(config-router)# address-family ipv4 unicast vrf red autonomous-system 1
Device(config-router-af)# topology base
Device(config-router-af-topology)# redistribute vrf global bgp 50000 metric 1000000 10 255
 1 1500
```

The following example shows how to redistribute global VRF routes into VRF BGP that were replicated from global BGP to Service VPN:

```
Device(config)# vrf definition 102
Device(config-vrf)# address-family ipv4
Device(config-ipv4)# route-replicate from vrf 102 unicast global bgp 50000
Device(config-ipv4)# exit-address-family
Device(config-vrf)# exit
Device(config)# router bgp 50000
Device(config-router)# ! Redistribute routes that were replicated from service vrf to bgp.
Device(config-router)# address-family ipv4 vrf 102
Device(config-router-af-topology)# redistribute vrf global bgp 50000 route-map BGP-route-map
```

The following example shows how to redistribute global VRF routes into VRF OSPF that were replicated from global BGP into VRF:

```
Device(config)# vrf definition 2
Device(config-vrf)# address-family ipv4
Device(config-ipv4)# route-replicate from vrf global unicast bgp 77
Device(config-ipv4)# exit-address-family
Device(config-vrf)# exit
Device(config)# router ospf 1 vrf test
Device(config-router)# ! Redistribute routes that were replicated from vrf global into ospf.
Device(config-router)# redistribute vrf global bgp 77
```

The following example shows how to redistribute routes via OSPF that were replicated from VRF 1:

```
Device(config)# vrf definition 2
Device(config-vrf)# rd 1:2
Device(config-vrf)# address-family ipv4
Device(config-ipv4)# route-replicate from vrf 1 unicast static route-map VRF1_TO_VRF2
Device(config-ipv4)# exit-address-family
Device(config)# router ospf 2 vrf 2
Device(config-router)# redistribute vrf 1 static route-map VRF1_TO_VRF2
```

route-replicate (VRF address family)

To replicate routes from another topology and Virtual Routing and Forwarding (VRF), use the **route-replicate** command in VRF address-family configuration mode. To stop replicating routes, use the **no** form of this command.

route-replicate from vrf *source-vrf-name* **unicast** *protocol* [**route-map** *map-tag*]
no route-replicate from vrf *source-vrf-name* **unicast** *protocol* [**route-map** *map-tag*]

Syntax Description

from	Specifies the topology where route replication is enabled.
vrf *source-vrf-name*	Specifies the name of the VRF from which routes are replicated.
unicast	Specifies a unicast SAFI.
protocol	Type of protocol of the source route. Some keywords require an argument. Valid keywords and arguments are: • **bgp** *autonomous-system-number*: Border Gateway Protocol (BGP). • **connected**: Connected routes. • **eigrp** *autonomous-system-number*: Enhanced Interior Gateway Routing Protocol (EIGRP). • **ospf** *process-id*: Open Shortest Path First (OSPF). • **static**: Static routes.
route-map *map-tag*	(Optional) Specifies the name of a route map that filters routes that shouldn't be replicated.

Command Default

No routes are replicated.

Command Modes

VRF address family configuration (config-ipv4)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	Support for route replication between service VPNs at the same edge device site.

Usage Guidelines

Route replication creates a link to a route in a routing information base (RIB) that is in a different VRF.

Examples

The following example redistributes global VRF BGP routes into VRF EIGRP that were replicated from VRF global into 1:

```
Device(config)# vrf definition 1
Device(config-vrf)# address-family ipv4
Device(config-ipv4)# route-replicate from vrf global unicast bgp 56
Device(config-ipv4)# exit-address-family
Device(config-vrf)# exit
Device(config)# router eigrp test
Device(config-router)# ! Redistribute routes that were replicated from vrf global into
eigrp.
Device(config-router)# address-family ipv4 unicast vrf red autonomous-system 1
Device(config-router-af)# topology base
Device(config-router-af-topology)# redistribute vrf global bgp 56
```

The following example redistributes global VRF EIGRP routes into BGP that were replicated from VRF global:

```
Device(config)# vrf definition 1
Device(config-vrf)# address-family ipv4
Device(config-ipv4)# route-replicate from vrf global unicast eigrp 56
Device(config-ipv4)# exit-address-family
Device(config-vrf)# exit
Device(config)# router bgp test
Device(config-router)# address-family ipv4 unicast vrf 10
Device(config-router-af)# redistribute vrf global bgp 56
Device(config-router-af)# exit-address-family
```

The following example shows how to redistribute routes via OSPF that were replicated from VRF 1 into VRF 2:

```
Device(config)# vrf definition 2
Device(config-vrf)# rd 1:2
Device(config-vrf)# address-family ipv4
Device(config-ipv4)# route-replicate from vrf 1 unicast static route-map VRF1_TO_VRF2
Device(config-ipv4)# exit-address-family
Device(config)# router ospf 2 vrf 2
Device(config-router)# redistribute vrf 1 static route-map VRF1_TO_VRF2
```

route-target

To create a route-target extended community for a Virtual Private Network (VPN) routing and forwarding (VRF) instance, use the **route-target** command in VRF configuration or in VRF address family configuration mode. To disable the configuration of a route-target community option, use the **no** form of this command.

route-target [**export** | **import**] *route-target-ext-community*

no route-target [**export** | **import**] *route-target-ext-community*

Syntax Description

import	(Optional) Imports routing information from the target VPN extended community.
export	Optional) Exports routing information to the target VPN extended community.
route-target-ext-community	The route-target extended community attributes to be added to the VRF's list of import, export, or both (import and export) route-target extended communities.

Command Default

A VRF has no route-target extended community attributes associated with it.

Command Modes

VRF definition configuration mode (config-vrf)

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For the usage guideline, see route-target

Examples

```
Device(config)# vrf definition 1
Device(config-vrf)# default route-target export 101:3
```

```
Device(config)# vrf definition 1
Device(config-vrf)# default route-target import 102:3
```

service tcp-keepalives-in

To generate keepalive packets on idle incoming network connections (initiated by the remote host), use the **service tcp-keepalives-in** command in global configuration mode . To disable the keepalives, use the **no**form of this command.

service tcp-keepalives-in
no service tcp-keepalives-in

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Command qualified for use in Cisco vManage CLI templates.

Examples

In the following example, keepalives on incoming TCP connections are generated:

```
Device(config)# service tcp-keepalives-in
```

service tcp-keepalives-out

To generate keepalive packets on idle outgoing network connections (initiated by a user), use the **service tcp-keepalives-out** command in global configuration mode . To disable the keepalives, use the **no**form of this command.

service tcp-keepalives-out
no service tcp-keepalives-out

Syntax Description This command has no arguments or keywords.

Command Default Disabled

Command Modes Global configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Command qualified for use in Cisco vManage CLI templates.

Examples

In the following example, keepalives on outgoing TCP connections are generated:

```
Device(config)# service tcp-keepalives-out
```

service tcp-small-servers

To enable small TCP servers such as the Echo, use the **service tcp-small-servers** command in global configuration mode. To disable the TCP server, use the **no** form of this command.

service tcp-small-servers
no service tcp-small-servers

Command Default TCP small servers are disabled.

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines For usage guidelines, see the Cisco IOS XE service tcp small servers command.

Examples The following example shows how to enable small TCP servers:

```
Device(config)# service tcp-small-servers
```

service udp-small-servers

To enable small User Datagram Protocol (UDP) servers such as the Echo, use the **service udp-small-servers** command in global configuration mode. To disable the UDP server, use the **no** form of this command.

service udp-small-servers
no service udp-small-servers

Command Default UDP small servers are disabled.

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines For usage guidelines, see the Cisco IOS XE service udp small servers command.

Examples The following example shows how to enable small UDP:

```
Router(config)# service udp-small-servers
```

vrf definition

To configure a virtual routing and forwarding (VRF) routing-table instance and enter VRF configuration mode, use the **vrf definition** command in global configuration mode. To remove a VRF routing table, use the **no** form of this command.

vrf definition *vrf-number*
no vrf definition *vrf-number*

Syntax Description

vrf-number	Number assigned to a VRF.

Command Default No VRFs are defined. No import or export lists are associated with a VRF. No route maps are associated with a VRF.

Command Modes Global configuration (config)

Command History

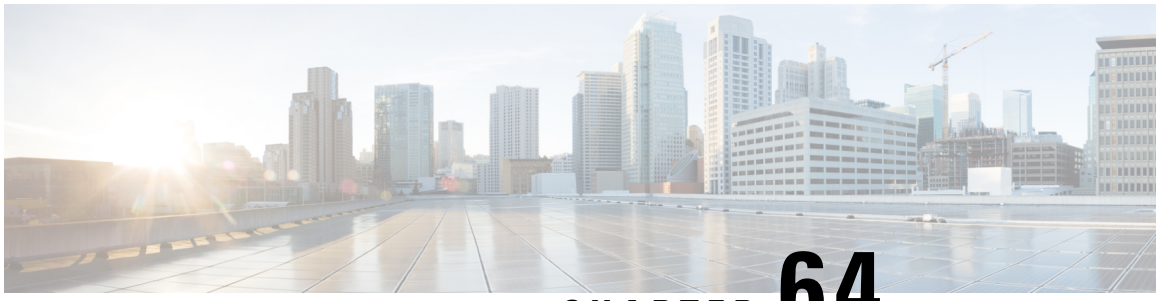
Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For the usage guideline, see vrf definition

Examples

```
Device(config)# vrf definition 1
```



CHAPTER 64

VRRP Commands

- object (tracking), on page 943
- track interface, on page 944
- track list, on page 945
- track (VRRP), on page 947
- track service, on page 948
- tloc-change increase-preference, on page 948
- vrf forwarding, on page 949
- vrrp address-family, on page 950

object (tracking)

To specify an object for a tracked list, use the **object** command in tracking configuration mode. To remove the object from the tracked list, use the **no** form of this command.

object *object-number* [**not**]
no object *object-number*

Syntax Description

object-number	Specifies the tracked object number in a tracked list. The range is from 1–1000.
not	(Optional) Negates the state of an object. **Note** The **not** keyword can be used in a Boolean list.

Command Default

The object isn't included in the tracked list.

Command Modes

Tracking configuration (config-track)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE object (tracking) command.

Examples

The following example shows two serial interfaces (objects) that are in tracked list 100. The Boolean "not" negates the state of object 2, resulting in the tracked list regarding object 2 as down when it's up:

```
Device(config)# track 1 interface serial2/0 line-protocol
Device(config-track)# exit
Device(config)# track 2 interface serial2/1 line-protocol
Device(config-track)# exit
Device(config)# track 100 list boolean and
Device(config-track)# object 1
Device(config-track)# object 2 not
```

track interface

To track an interface and to enter tracking configuration mode, use the **track interface** command in global configuration mode. To remove the tracking, use the **no** form of this command.

track *object-number* **interface** [**carrier-delay** | **delay** | **endpoint-tracker** | **interface** | **ip** | **ipv6** | **list** | **service** | **stub-object** | **threshold**] [**line-protocol** | **ip routing** | **ipv6 routing**]

no track *object-number*

Syntax Description

object-number	Specifies the object number that represents the interface to be tracked. The range is from 1–1000.
[carrier-delay | delay | endpoint-tracker | interface | ip | ipv6 | list | service | stub-object | threshold]	(Optional) Specifies the interface type to be tracked.
line-protocol	Tracks the state of the interface line protocol.
ip routing	Tracks whether IP routing is enabled, whether an IP address is configured on the interface, and whether the interface state is up before reporting to the tracking client that the interface is up.
ipv6 routing	Tracks whether IPv6 routing is enabled, whether an IPv6 address is configured on the interface, and whether the interface state is up before reporting to the tracking client that the interface is up.

Command Default

No interface is tracked.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE track interface command.

Examples

The following example shows how to configure the tracking process to track the IP-routing capability of serial interface 1/0:

```
Device(config)# track 1 interface serial1/0 ip routing
Device(config-track)# exit
```

The following example shows how to configure the tracking process to track the IPv6-routing capability of a GigabitEthernet interface 1/0/0:

```
Device(config)# track 1 interface GigabitEthernet 1/0/0 ipv6 routing
Device(config-track)# exit
```

The following example shows how to configure two tracker and adding them to the track list using the boolean 'and' operation:

```
Device# config-transaction
Device(config)# track 100 interface GigabitEthernet2 line-protocol
Device(config-track)# exit
Device(config)# track 200 interface GigabitEthernet3 line-protocol
Device(config-track)# exit
Device(config)# track 400 list boolean and
Device(config-track)# object 100
Device(config-track)# object 200
Device(config-track)# exit
```

track list

To specify a list of objects to be tracked and the thresholds to be used for comparison, use the **track list** command in global configuration mode. To disable the tracked list, use the **no** form of this command.

track *object-number* **list** {**boolean** {**and** | **or**} | **threshold** {**weight** | **percentage**}}
no track *object-number* **list** {**boolean** {**and** | **or**} | **threshold** {**weight** | **percentage**}}

Syntax Description

object-number	Object number of the object to be tracked. The range is from 1–1000.
boolean	State of the tracked list is based on a boolean calculation. The keywords are as follows: • **and** : Specifies that the list is “up” if all objects are up, or “down” if one or more objects are down. For example when tracking two interfaces, “up” means that both interfaces are up, and “down” means that either interface is down. • **or** : Specifies that the list is “up” if at least one object is up. For example, when tracking two interfaces, “up” means that either interface is up, and “down” means that both interfaces are down.
threshold	State of the tracked list is based on a threshold. The keywords are as follows: • **percentage** : Specifies that the threshold is based on a percentage. • **weight** : Specifies that the threshold is based on a weight.

Command Default

The object list is not tracked.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE track list command.

Examples

The following example shows how to configure a track list object to track two GigabitEthernet interfaces:

```
Device(config)# track 1 interface GigabitEthernet2 line-protocol
Device(config-tracker)# exit
Device(config)# track 2 interface GigabitEthernet3 line-protocol
Device(config-tracker)# exit
Device(config)# track 100 list boolean and
Device(config-tracker)# object 1
Device(config-tracker)# object 2
Device(config-tracker)# exit
```

The following configurations provide some hysteresis in case one of the serial interfaces is flapping.

The following example shows how to configure a track list object to track two serial interfaces when both serial interfaces are “up” and when either serial interface is “down”:

```
Device(config)# track 1 interface serial2/0 line-protocol
Device(config-track)# exit
Device(config)# track 2 interface serial2/1 line-protocol
Device(config-track)# exit
Device(config)# track 100 list boolean and
Device(config-track)# object 1
Device(config-track)# object 2
```

The following example shows how to configure a track list object to track two serial interfaces when either serial interface is “up” and when both serial interfaces are “down”:

```
Device(config)# track 1 interface serial2/0 line-protocol
Device(config-track)# exit
Device(config)# track 2 interface serial2/1 line-protocol
Device(config-track)# exit
Device(config)# track 101 list boolean or
Device(config-track)# object 1
Device(config-track)# object 2
```

The following example shows how to configure a track list object to track two serial interfaces when both serial interfaces are “up” and when both serial interfaces are “down,” for example:

```
Device(config)# track 1 interface serial2/0 line-protocol
Device(config-track)# exit
Device(config)# track 2 interface serial2/1 line-protocol
Device(config-track)# exit
Device(config)# track 102 threshold weight
Device(config-track)# object 1 weight 10
Device(config-track)# object 2 weight 10
Device(config-track)# threshold weight up 20 down 0
```

track (VRRP)

To enable an object to be tracked using a Virtual Router Redundancy Protocol version 3 (VRRPv3) group, use the **track** command in VRRP configuration mode. To disable the tracking, use the **no** form of this command.

track *object-number* { **shutdown** | [**decrement** *priority*] }
no track *object-number* **shutdown**

Syntax Description

object-number	Object number representing the interface to be tracked. The range is from 1–1000.
shutdown	Shuts down the VRRPv3 group.
decrement *priority*	Sets the priority value by which the VRRP group is reduced if the tracked object state on serial interface VRRPv3 goes down. The valid range is 1–255.

Command Default

Tracking an object using a VRRPv3 group isn't enabled.

Command Modes

VRRP configuration (config-if-vrrp)

Command History

Release	Modification
Cisco IOS XE Release Amsterdam 17.2.1v	Qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For the usage guidelines, see track (VRRP).

Examples

The following example shows how to configure VRRPv3 group shutdown:

```
Device(config)# interface GigabitEthernet1
Device(config-if)# vrrp 2 address-family ipv4
Device(config-if-vrrp)# track 2 shutdown
```

The following example shows how to configure the tracking process to track the state of the IPv6 object using the VRRPv3 group. VRRP on GigabitEthernet interface 0/0/0 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
```

The following example shows how to configure the tracking process to track the state of the IPv4 object. VRRP on GigabitEthernet2 registers with the tracking process to be informed of any changes to the IPv4 object. If the IPv4 object state on interface goes down, then the priority of the VRRP group is reduced by 10:

```
Device(config)# interface GigabitEthernet2
Device(config-if)# ip address 10.10.1.1 255.255.255.0
Device(config-if)# negotiation auto
Device(config-if)# vrrp 1 address-family ipv4
Device(config-if-vrrp)# address 10.10.1.10 primary
Device(config-if-vrrp)# track 400 decrement 10
```

```
Device(config-if-vrrp)# tloc-change increase-preference 1
Device(config-if-vrrp)# exit
```

track service

To configure track list and tracking for SIG containers, use the **track service** command in global configuration mode. To disable the configuration, use the **no** form of this command.

track *object-number* **service** *string*
no track *track-number* **service**

Syntax Description

string	(Optional)
object-number	Specifies the object number that represents the interface to be tracked. The range is from 1–1000.

Command Default

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

Examples

The following example shows how to configure track list and tracking for SIG containers:

```
Device(config)# track 1 service global
Device(config-track)# exit
Device(config)# track 2 service global
Device(config-track)# exit
Device(config)# track 3 list boolean and
Device(config-track)# object 100
Device(config-track)# object 200
Device(config-track)# exit
```

tloc-change increase-preference

To configure tloc-change preference value, use the **tloc-change increase-preference** command in VRRP interface configuration mode. To disable the configuration, use the **no** form of this command.

tloc-change increase-preference *value*
no tloc-change

Syntax Description

value	Specifies the TLOC change preference configuration under VRRP group. The value increases by one when a node becomes the primary node. Range: 1–4294967295.

Command Default

Command Modes

VRRP Interface configuration (config-if-vrrp)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

The default value for tloc-change increase-preference value is one.

We recommend that you use the same TLOC preference value for all TLOCs in a site. For a Cisco vEdge device, the default TLOC preference for the tunnel interface can be modified irrespective of whether VRRP is configured or not. However, if you want to use the VRRP tracking feature and utilize the advantage of TLOC preference values for VRRP tracking, ensure that the default tunnel preference is same on both the VRRP routers.

Examples

The following example shows how to configure TLOC change preference value:

```
Device(config)# interface GigabitEthernet2
Device(config-if)# vrf forwarding 1
Device(config-if)# ip address 10.10.1.1 255.255.255.0
Device(config-if)# negotiation auto
Device(config-if)# vrrp 1 address-family ipv4
Device(config-if-vrrp)# address 10.10.1.10 primary
Device(config-if-vrrp)# track 400 decrement 10
Device(config-if-vrrp)# tloc-change increase-preference 1
Device(config-if-vrrp)# exit
```

vrf forwarding

To associate a VRF instance or a virtual network with an interface or subinterface, use the **vrf forwarding** command in interface configuration mode. To disassociate a VRF or virtual network from an interface or subinterface, use the **no** form of this command.

vrf forwarding *vrf-name*
no vrf forwarding *vrf-name*

Syntax Description

vrf-name	The VRF name to be associated with the specified interface.

Command Default

The default for an interface is the global routing table.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For the usage guidelines, see vrf forwarding.

Examples

```
Device(config)# interface GigabitEthernet 1
Device(config-if)# vrf forwarding vrf1
```

vrrp address-family

To create a VRRP group and to enter VRRP configuration mode, use the **vrrp address-family** command in interface configuration mode. To remove the VRRP group, use the **no** form of this command.

vrrp *group* **address-family** { **ipv4** | **ipv6** }
no vrrp *group* **address-family** { **ipv4** | **ipv6** }

Syntax Description

group	VRRP group number ranges from 1 to 255.
ipv4	Enter VRRP IPv4 address-family configuration.
ipv6	Enter VRRP IPv6 address-family configuration.

Command Default

None

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Use the **vrrp address-family** command to create a VRRP group and to enter VRRP configuration mode. VRRP is the only FHRP (First Hop Redundancy Protocol) supported by Cisco Catalyst SD-WAN edge routers in controller mode. Once you create the group and specify the address-family, you can configure different settings for VRRP.

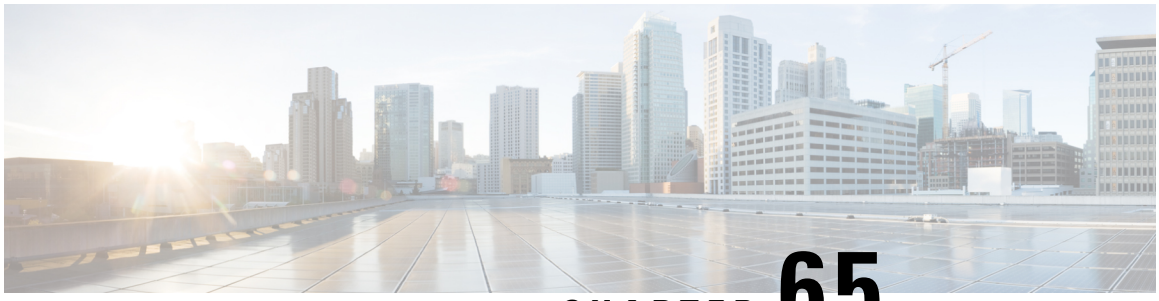
Examples

The following example creates and customizes VRRP group 3:

```
Device# config-transaction
Device(config)# int GigabitEthernet0/0/2
Device(config-if)# vrrp 3 address-family ipv4
```

Table 70: Related Commands

Command	Description
address primary (VRRP)	Configures a primary IP address for VRRP.



CHAPTER 65

Zone Based Firewall Commands

- alert (zone-based policy), on page 951
- app-visibility, on page 952
- class-map, on page 953
- class-map type inspect, on page 954
- class (policy-map), on page 955
- drop, on page 956
- flow-visibility, on page 957
- implicit-acl-logging, on page 958
- inspect, on page 958
- log (parameter-map type), on page 959
- log flow-export, on page 959
- log-frequency, on page 960
- match access-group, on page 961
- multi-tenancy, on page 961
- parameter-map type inspect-global, on page 962
- policy, on page 963
- policy-map type inspect, on page 965
- service-policy (zones), on page 966
- service-policy type inspect, on page 966
- vpn zone security, on page 967
- vpn (zone), on page 968
- zone pair security, on page 968
- zone security, on page 969

alert (zone-based policy)

To turn on or off console display of Cisco IOS stateful packet inspection alert messages, use the **alert** command in parameter-map type inspect configuration mode. To change the configured setting or revert to the default setting, use the **no** form of this command.

alert on
no alert

Syntax Description

on	Enables message logging for instant messenger application policy events.

Command Default

Alert messages are not issued.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE alert (zone-based policy) command.

Examples

```
Router(config)# parameter-map type inspect insp-params
Router(config-profile)# alert on
```

```
Router(config)# parameter-map type inspect-global
Router(config-profile)# alert on
```

app-visibility

To enable application visibility so that a router can monitor and track the applications running on the LAN use the **app-visibility** command. Use the **no** form of this command to disable application visibility.

app-visibility

Command Default

Disabled.

Command Modes

Policy configuration (config-policy)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

To enable NBAR feature to recognize applications. Use the **show sdwan app-fwd dpi** command to see DPI flows.

Examples

Enable application-visibility on a router:

```
Router(config)# policy
Router(config-policy)# app-visibility
```

class-map

To create a class map to be used for matching packets to a specified class and to enter QoS class-map configuration mode, use the **class-map** command in global configuration mode. To remove an existing class map from a device, use the **no** form of this command.

class-map { [**type inspect match-all**] | [**match-any**] } *class-map-name*
no class-map { [**type inspect match-all**] | [**match-any**] }

Syntax Description

type inspect	(Optional) Specifies the class-map type as inspect.
match-all	(Optional) Determines how packets are evaluated when multiple match criteria exist. Matches statements under this class map based on the logical AND function. A packet must match all statements to be accepted. If you do not specify the **match-all** or **match-any** keyword, the default keyword used is **match-all**.
match-any	(Optional) Determines how packets are evaluated when multiple match criteria exist. Matches statements under this class map based on the logical OR function. A packet must match any of the match statements to be accepted. If you do not specify the **match-any** or **match-all** keyword, the default keyword is used **match-all**.
class-map-name	Name of the class for the class map. The class name is used for both the class map and to configure a policy for the class in the policy map. **Note** You can enter the value for the *class-map-name* argument within quotation marks. The software does not accept spaces in a class map name entered without quotation marks.

Command Default

A class map is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `class-map` command.

Examples

```
class-map match-any BestEffort
  match qos-group 3
 !
 class-map match-any Bulk
  match qos-group 4
 !
 class-map match-any Critical
  match qos-group 1
 !
 class-map match-any Critical-Low
```

```
 match qos-group 2
!
class-map match-any BULK
 match qos-group 2
!
class-map match-any CONTROL-SIGNALING
 match qos-group 4
!
class-map match-any CRITICAL-DATA
 match qos-group 1
!
class-map match-any Default
 match qos-group 5
!
class-map match-any INTERACTIVE-VIDEO
 match qos-group 3
!
class-map match-any LLQ
 match qos-group 0
!
class-map match-any Queue0
 match qos-group 0
!
class-map match-any Queue1
 match qos-group 1
!
class-map match-any Queue2
 match qos-group 2
!
class-map match-any Queue3
 match qos-group 3
!
class-map match-any Queue4
 match qos-group 4
!
class-map match-any Queue5
 match qos-group 5
!
class-map type inspect match-all cmap
 match access-group name cmap
!
class-map match-any Queue4
 match qos-group 0
!
```

The following example configures the match criterion for a class map on the basis of a specified protocol for zone based policy firewall:

```
class-map match-any aa1-cm0_
match protocol test
match protocol mpeg2-ts
!
```

class-map type inspect

To create a Layer 3 and Layer 4 or a Layer 7 (application-specific) inspect type class map, use the **class-map type inspect** command in global configuration mode. To remove a class map from the router configuration file, use the **no** form of this command.

Layer 3 and Layer 4 (Top Level) Class Map Syntax
class-map type inspect {**match-any** | **match-all**} *class-map-name*
no class-map type inspect {**match-any** | **match-all**} *class-map-name*

Layer 7 (Application-Specific) Class Map Syntax
class-map type inspect { **match-any** | **match-all** } *class-map-name*
no class-map type inspect { **match-any** | **match-all** } *class-map-name*

Syntax Description

match-any	Determines how packets are evaluated when multiple match criteria exist. Packets must meet one of the match criteria to be considered a member of the class.
match-all	Determines how packets are evaluated when multiple match criteria exist. Packets must meet all of the match criteria to be considered a member of the class. **Note** The **match-all** keyword is available only with Layer 3, Layer 4, and SMTP type class maps.
class-map-name	Name of the class map. The name can have a maximum of 40 alphanumeric characters. The class map name is used to configure the policy for the class in the policy map.

Command Default

The behavior of the **match-any** keyword is the default.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE class-map type inspect command.

Examples

```
class-map type inspect match-any test-sRule_2-l4-cm_
match protocol tcp
match protocol udp
!
class-map type inspect match-all test-seq-1-cm_
match access-group name test-seq-Rule_1-acl_
!
class-map type inspect match-all test-seq-11-cm_
match class-map test-sRule_2-l4-cm_
!
```

class (policy-map)

To specify the name of the class whose policy you want to create or change or to specify the default class (commonly known as the class-default class) before you configure its policy, use the **class**command in policy-map configuration mode. To remove a class from the policy map, use the **no** form of this command.

class { *class-name* | **class-default** }
no class { *class-name* | **class-default** }

Syntax Description

class-name	Name of the class to be configured or whose policy is to be modified. The class name is used for both the class map and to configure a policy for the class in the policy map.
class-default	Specifies the default class so that you can configure or modify its policy.

Command Default

No class is specified.

Command Modes

Policy-map configuration (config-pmap)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `class (policy-map)` command.

Examples

The following example shows how to create two policy maps called “PMap” and "generic-cos" and configure two class policies in each policy map.

```
policy-map PMap
 class PMap-super-fast
  priority level 1
  police percent 5
 !
 class PMap-fast
  priority level 2
  police percent 5
 !
!
policy-map generic-cos
 class cos-map-generic
  bandwidth remaining percent 5
  queue-limit 108 packets
 !
 class class-default
  bandwidth remaining percent 95
  queue-limit 2028 packets
 !
!
```

drop

To configure a traffic class to discard packets belonging to a specific class, use the **drop** command in policy-map class configuration mode. To disable the packet discarding action in a traffic class, use the **no** form of this command.

drop

no drop

Syntax Description This command has no arguments or keywords.

Command Default Disabled

Command Modes

Policy-map class configuration (config-pmap-c)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Examples

```
policy-map shape_GigabitEthernet0/0/1
  class class-default
   service-policy Branch-QoS-Policy
   shape average 1000000000
  !
  class class-default
    drop
  !
 !


policy-map type inspect test101
  class test101-seq-11-cm_
  drop
  !
```

flow-visibility

To enable flow visibility so that a router can perform traffic flow monitoring on traffic coming to the router from the LAN use the **flow-visibility** command. To disable the flow visibility use the **no** form of this command.

flow-visibility

no flow-visibility

Command Default Disabled.

Command Modes

Policy configuration (config-policy)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines Use the **show sdwan app-fwd cflowd** command to enable cflowd flow monitoring.

Examples

The following is an example of this command

```
Router(config)# policy
Router(config-policy)# flow-visibility
```

implicit-acl-logging

To configure your Cisco IOS XE Catalyst SD-WAN device to log dropped packets in the traffic, use the **implicit-acl-logging** command.

implicit-acl-logging

no implicit-acl-logging

Command Default

Logging is disabled.

Command Modes

Policy configuration (config-policy)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

You can use these logs for security purposes; for example, to monitor the flows that are being directed to a WAN interface and to determine, in the case of a DDoS attack, which IP addresses to block.

When you enable implict ACL logging, by default, every 512th packet per flow is logged. It is recommended that you limit the number of packets logged, by including the **log-frequency** command in the configuration.

Log implicitly configured packets, logging every 512th packet per flow:

```
Router(config)# Policy
Router(config-policy)# implicit-acl-logging
```

inspect

To enable Cisco IOS stateful packet inspection, use the **inspect** command in policy-map-class configuration mode. To disable stateful packet inspection, use the **no** form of this command.

inspect
no inspect

Command Default

Cisco IOS stateful packet inspection is disabled.

Command Modes

Policy-map-class configuration (config-pmap-c)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE inspect command.

Examples

The following example specifies inspection parameters and requests the **inspect** action with the specified inspect parameter:

```
policy-map type inspect mypolicy
 class type inspect inspect-traffic
  inspect
```

log (parameter-map type)

To log the firewall activity for an inspect parameter map, use the **log** command in parameter-map type inspect configuration mode.

log dropped-packets

Syntax Description

dropped-packets	Logs the packets dropped by the firewall.

Command Default

The firewall activity is not captured.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE log (parameter-map type) command.

Examples

The following example show how to configure the packets dropped by the firewall.

```
Router(config)# parameter-map type inspect-global
Router(config-profile)# alert on
Router(config-profile)# log dropped-packets
```

log flow-export

To log firewall events in NetFlow Version 9 format to an external netflow collector, use the **log flow-export** command in parameter-map type inspect-global configuration mode.

log flow-export

Syntax Description

v9	Specifies NetFlow Version 9 export as the export protocol.
udp	Configures the UDP connection.
destination	Specifies an IPv4 address destination.
ipv6-destination	Specifies an IPv6 address destination.
source	The source interface the device for HSL.

Command Modes

Parameter-map type inspect-global configuration (config-profile)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Examples

The following example show how to configure logging of of firewall events in NetFlow Version 9 format to an external IP address:

```
Device(config)# parameter-map type inspect-global
Device(config-profile)# log flow-export v9 udp destination 10.0.2.0 5000 vrf 1 source
GigabitEthernet0/0/5
Device(config-profile)# log flow-export v9 udp ipv6-destination 2001:DB8::1 vrf 65528 source
 GigabitEthernet0/0/3
```

log-frequency

To configure how often packet flows are logged, use the **log-frequency** command.

log-frequency *number*

Syntax Description

number	Logging Frequency: How often packet flows are logged. Range: Any positive integer value. While you can configure any positive integer value for the frequency, the software rounds the value down to the nearest power of 2. Default: 1000. With this default, the logging frequency is rounded down to 512. So, by default, every 512th packet per flow is logged. Maximum value: 2147483647

Command Default

Default logging frequency: 512

Command Modes

Policy configuration (config-policy)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

The following is an example of this command:

```
Router(config)# Policy
Router(config-policy)# implicit-acl-logging
Router(config-policy)# log-frequency 1000
```

match access-group

To configure the match criteria for a class map on the basis of the specified access control list (ACL), use the **match access-group** command in class-map configuration mode. To remove ACL match criteria from a class map, use the **no** form of this command.

match access-group name *access-group-name*
no match access-group name *access-group-name*

Syntax Description

name *access-group-name*	Named ACL whose contents are used as the match criteria against which packets are checked to determine if they belong to this class. The name can be a maximum of 40 alphanumeric characters.

Command Default

No match criterion is specified.

Command Modes

QoS class-map configuration (config-cmap)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Examples

```
class-map type inspect match-all cmap
  match access-group name cmap
 !
```

multi-tenancy

To enable multi-tenancy as a global parameter map, use the **multi-tenancy** command in parameter-map type inspect configuration mode. To disable multi-tenancy as a global parameter map, use the **no** form of this command.

multi-tenancy

no multi-tenancy

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Parameter-map type inspect configuration (config-profile).

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines A parameter map allows you to specify parameters that control the behavior of actions and match criteria sthat are specified under a policy map and a class map respectively, for zone-based firewall policies.

Examples The following example shows how to enable multi-tenancy as a global parameter map:

```
Device(config)# parameter-map type inspect-global
Device(config-profile)# multi-tenancy
```

parameter-map type inspect-global

To configure a global parameter map and enter parameter-map type inspect configuration mode, use the **parameter-map type inspect-global** command in global configuration mode. To delete a global parameter map, use the **no** form of this command.

parameter-map type inspect-global
no parameter-map type inspect-global

Syntax Description This comand has no keywords or arguments.

Command Default Global parameter maps are not configured.

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines After you enter the **parameter-map type inspect-global** command, you can enter the commands listed in the table below in parameter-map type inspect-global configuration modes.

Command	Description
aggressive-aging	Enables aggressive aging of half-opened firewall sessions.
alert on	Enables Cisco IOS stateful packet inspection alert messages.

Command	Description
inspect	Enables and disables audit trail messages.
log {**dropped-packets** | **flow-export**}	Logs the dropped packets.
max-incomplete {**low** | **high**} *number-of-connections*	Defines the number of existing half-open sessions that will cause the software to start and stop deleting half-open sessions.
multi-tenancy	Enables Cisco vManage for multitenancy.
vpn zone security	Inspects traffic exchange between multiple service VPNs.

Ensure that you configure the **parameter-map type inspect-global** command with **vpn zone security** command to enable zone-based firewall.

For more information on usage guidelines, see the Cisco IOS XE parameter-map type inspect-global command.

Examples

The following example shows a sample parameter-map type inspect-global configuration:

```
Device(config)# parameter-map type inspect-global
Device(config)# alert on
Device(config-profile)# log dropped-packets
Device(config-profile)# multi-tenancy
Device(config-profile)# vpn zone security allow dia
```

policy

To enter policy configuration mode or configure policies, use the **policy** command in global configuration mode. To remove policy configurations, use the **no** form of this command.

policy [**access-list** | **app-visibility** | **class-map** | **cloud-qos-service-side** | **flow-visibility** | **flow-stickiness-disable** | **implicit-acl-logging** | **ipv6** | **lists** | **log-frequency** | **mirror** | **policer** | **qos-map** | **qos-scheduler** | **rewrite-rule** | **route-policy** | **utd-tls-decrypt**]
no policy [**access-list** | **app-visibility** | **class-map** | **cloud-qos-service-side** | **flow-visibility** | **implicit-acl-logging** | **ipv6** | **lists** | **log-frequency** | **mirror** | **policer** | **qos-map** | **qos-scheduler** | **rewrite-rule** | **route-policy** | **utd-tls-decrypt**]

Syntax Description

access-list	(Optional) Configures ACLs.
app-visibility	(Optional) Enables/disables application visibility.
class-map	(Optional) Configures class map.
cloud-qos	(Optional) Enables/Disables QoS for cEdge Cloud.
cloud-qos-service-side	(Optional) Enables/Disables QoS for cEdge Cloud on service side.
flow-visibility	(Optional) Enables/Disables flow visibility.
flow-stickiness-disable	(Optional) Enables/Disables flow stickiness.

implicit-acl-logging	(Optional) Enables/Disables logging of implicit acl packet drops.
ipv6	(Optional) Configures IPv6 policy.
lists	(Optional) Configures lists.
log-frequency	(Optional) Logs frequency as packet counts.
mirror	(Optional) Configures traffic mirror.
policer	(Optional) Configures policer.
qos-map	(Optional) Configures QoS map.
qos-scheduler	(Optional) Configures QoS scheduler.
rewrite-rule	(Optional) Configures rewrite rule.
route-policy	(Optional) Configures route policies
utd-tls-decrypt	(Optional) Configures TLS Decryption policies.

Command Default

Default behavior or values vary based on optional arguments or keywords.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.
Cisco IOS XE Release 17.6.1a	The **flow-stickiness-disable** keyword is added.
Cisco IOS XE Catalyst SD-WAN Release 17.13.1a	The **flow-stickiness-disable** keyword is added for NAT66 DIA.

Usage Guidelines

Policy influences the flow of data traffic and routing information among Cisco devices in the overlay network. This command can be used to enter the policy configuration mode where further configurations can be done or to configure policies with optional arguments or keywords.

Example

The following example enters the policy configuration mode. It defines a policer profile named pol1 and sets the burst size to 15,000 bytes, and rate to 500,000,000 bps, and configures to drop the traffic if the burst size or traffic rate is exceeded.

```
Device(config)# policy
Device(config-policy)# policer pol1
Device(config-policy-pol1)# burst 15000
Device(config-policy-pol1)# rate 500000000
Device(config-policy-pol1)# exceed drop
Device(config-policy-pol1)# flow-stickiness disable
```

The following example enables app-visibility.

```
Device(config)# policy app-visibility
```

The following example disables flow-stickiness.

```
Device(config-policy)# flow-stickiness disable
```

policy-map type inspect

To create a Layer 3 and Layer 4 or a Layer 7 (protocol-specific) inspect-type policy map, use the **policy-map type inspect** command in global configuration mode. To delete an inspect-type policy map, use the **no** form of this command.

Layer 3 and Layer 4 (Top Level) Policy Map Syntax
policy-map type inspect *policy-map-name*
no policy-map type inspect *policy-map-name*

Layer 7 (Application-Specific) Policy Map Syntax
policy-map type inspect *protocol-name policy-map-name*
no policy-map type inspect *protocol-name policy-map-name*

Syntax Description

policy-map-name	Name of the policy map. The name can be a maximum of 40 alphanumeric characters.
protocol-name	Layer 7 application-specific policy map. The supported protocol is: **avc** —Firewall AVC-based poilcy map.

Command Default

No policy map is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE policy-map type inspect command.

Examples

```
policy-map type inspect avc aa1-pm_
! first
class aa1-cm0_
deny
```

service-policy (zones)

To attach a Layer 7 policy map to a top-level policy map, use the **service-policy** command in zone-pair configuration mode. To delete a Layer 7 policy map from a top-level policy map, use the **no** form of this command.

service-policy *policy-map-name*
no service-policy *policy-map-name*

Syntax Description

policy-map-name	Name of the Layer 7 policy map to be attached to a top-level policy map.

Command Default

None

Command Modes

Zone-pair configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE service-policy (zones) command.

Examples

```
policy-map type inspect test
class test-seq-1-cm_
inspect audit-trail-pmap_
service-policy avc aa1-pm_
!
```

service-policy type inspect

To attach a firewall policy map to a zone-pair, use the **service-policy type inspect** command in zone-pair configuration mode. To disable this attachment to a zone-pair, use the **no** form of this command.

service-policy type inspect *policy-map-name*
no service-policy type inspect *policy-map-name*

Syntax Description

policy-map-name	Name of the policy map. The name can be a maximum of 40 alphanumeric characters.

Command Default

None

Command Modes

Zone-pair configuration (config-sec-zone-pair)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE service-policy type inspect command.

Examples

The following example defines zone-pair LAN-WAN and attaches the service policy test-policy to the zone-pair:

```
!
zone security LAN
vpn 2
!
zone security WAN
vpn 0
!
zone-pair security ZP_LAN_WAN_test-policy source LAN destination WAN
 service-policy type inspect test-policy
!
```

vpn zone security

To enable vpn zone security globally, use the **vpn zone security** command under the **parameter-map type inspect-global** command mode for inspecting traffic between zones. To remove the vpn zone security, use the no form of the command under the parameter-map type inspect-global configuration mode.

vpn zone security

no vpn zone security

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command is qualified for use in Cisco vManage CLI templates.

Usage Guidelines

Zone-based firewall feature can be enabled on Cisco IOS XE Catalyst SD-WAN devices for inspecting traffic exchange between multiple service VPNs. This feature can be globally enabled by using the vpn zone security command under parameter-map type inspect-global command.

Examples

The following example shows enabling zone based firewall feature globally:

```
Device(config)# parameter-map type inspect-global
Device(config-profile)# vpn zone security
```

Related Commands

Command	Description
zone security	Defines a security zone.
zone-pair security	Defines a zone pair on which to implement the zone security firewall feature.

vpn (zone)

To associate a vpn with a zone , use the **vpn** *id* command under the **zone security** command. To disassociate a vpn id, use the **no** form under the **zone security** mode.

vpn *id*
no vpn *id*

Syntax Description

id	Specifies the id of a vrf configured on a Cisco IOS XE Catalyst SD-WAN device.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Zone-based firewall feature can be enabled on Cisco IOS XE Catalyst SD-WAN devices for inspecting traffic exchange between multiple service VPNs. This feature can be globally enabled by using the vpn zone security command under parameter-map type inspect-global command.

Examples

The following example shows how to associate vpn 32 with zone corporate:

```
Device(config)# zone security corporate
Device(config-sec-zone)# vpn 32
```

Related Commands

Command	Description
zone-pair security	Defines a zone-pair on which to implement the zone security firewall feature.

zone pair security

To create a zone pair, use the **zone-pair security** command in global configuration mode. To delete a zone pair, use the **no** form of this command.

zone-pair security *zone-pair-name* **source** [*source-zone-name* | **self**] **destination** [*destination-zone-name* | **self**]
no zone-pair security *zone-pair-name* **source** [*source-zone-name* | **self**] **destination** [*destination-zone-name* | **self**]

Syntax Description

zone-pair-name	Name of the zone being attached to an interface. You can enter up to 128 alphanumeric characters.
source *source-zone-name*	Specifies the name of the router from which traffic is originating.
destination *destination-zone-name*	Specifies the name of the device to which traffic is bound.
self	Specifies the system-defined zone. Indicates whether traffic will be going to or from a device.

Command Default

A zone pair is not created.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE zone-pair security command.

Examples

The following example shows how to create zones LAN and WAN, identify them, and create a zone pair where LAN is the source and WAN is the destination:

```
zone security LAN
vpn 2
!
zone security WAN
vpn 0
!
```

The following example shows how to define zone pair LAN-WAN and attach a service policy, test-policy to the zone-pair:

```
zone-pair security ZP_LAN_WAN_test-policy source LAN destination WAN
  service-policy type inspect test-policy
```

zone security

To create a security zone, use the **zone security** command in global configuration mode. To delete a security zone, use the **no** form of this command.

zone security *zone-name*
no zone security *zone-name*

Syntax Description

zone-name	Name of the security zone. You can enter up to 256 alphanumeric characters.

Command Default

There is a system-defined "self" zone.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

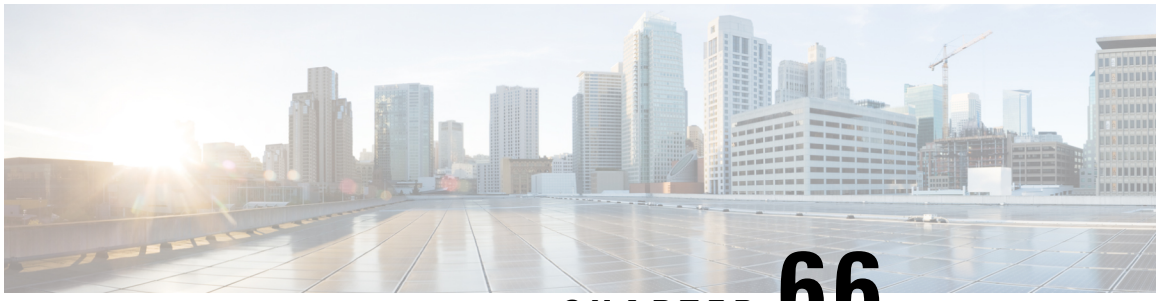
Note The self zone does not require any declaration.

For usage guidelines, see the Cisco IOS XE zone security command.

Examples

The following example shows how to create and describe zones LAN and WAN:

```
zone security LAN
 vpn 2
!
zone security WAN
 vpn 0
!
```



CHAPTER 66

Zscaler Commands

- aup, on page 971
- auth-required, on page 972
- caution-enabled, on page 973
- datacenters, on page 973
- ips-control, on page 974
- ofw-enabled, on page 974
- secure-internet-gateway, on page 975
- ssl-scan-enabled, on page 976
- surrogate display-time-unit, on page 977
- surrogate idle-time, on page 977
- surrogate ip, on page 978
- surrogate ip-enforced-for-known-browsers, on page 979
- surrogate refresh-time, on page 980
- surrogate refresh-time-unit, on page 980
- tunnel-options, on page 981
- xff-forward-enabled, on page 982
- zscaler-location-settings, on page 983

aup

To configure Zscaler acceptable user policy (AUP) parameters, use the **aup** command in zscaler location settings configuration (config-zscaler-location-settings) mode.

aup { **disabled** | **block-internet-until-accepted false** | **force-ssl-inspection false** | **timeout** *time* }

Syntax Description

disabled	Only this option is qualified for use.
block-internet-until-accepted false	Only the **false** option is qualified for use.
force-ssl-inspection false	Only the **false** option is qualified for use.
timeout *time*	Use the value 0.

Command Default

disabled

Command Modes zscaler location settings configuration (config-zscaler-location-settings)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

```
Device(config)# sdwan

Device(config-sdwan)# service sig vrf global
Device(config-vrf-global)# zscaler-location-settings
Device(config-zscaler-location-settings)# aup disabled
Device(config-zscaler-location-settings)# aup block-internet-until-accepted false
Device(config-zscaler-location-settings)# aup force-ssl-inspection false
Device(config-zscaler-location-settings)# aup timeout 0
```

auth-required

To configure Zscaler authentication, use the **auth-required** command in zscaler location settings configuration (config-zscaler-location-settings) mode. To disable Zscaler authentication, use the **no** form of this command.

auth-required false

no auth-required

Syntax Description

false	Disables the authentication. Only this option is qualified for use in Cisco SD-WAN Manager CLI templates.

Command Default This command is enabled by default.

Command Modes zscaler location settings configuration (config-zscaler-location-settings)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines The following example shows how to disable the authentication:

```
Device(config)# sdwan

Device(config-sdwan)# service sig vrf global
Device(config-vrf-global)# zscaler-location-settings
Device(config-zscaler-location-settings)# auth-required
Device(config-zscaler-location-settings)# auth-required false
```

caution-enabled

To enable or disable Zscaler caution notification, use the **caution-enabled** command in zscaler location settings configuration (config-zscaler-location-settings) mode.

caution-enabled false

Syntax Description

false	Only this option is qualified for use.

Command Default

false

Command Modes

zscaler location settings configuration (config-zscaler-location-settings)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

```
Device(config)# sdwan

Device(config-sdwan)# service sig vrf global
Device(config-vrf-global)# zscaler-location-settings
Device(config-zscaler-location-settings)# aup disabled
Device(config-zscaler-location-settings)# aup block-internet-until-accepted false
Device(config-zscaler-location-settings)# aup force-ssl-inspection false
Device(config-zscaler-location-settings)# aup timeout 0
Device(config-zscaler-location-settings)# caution-enabled false
```

datacenters

To configure Zscaler custom data centers, use the **datacenters** command in zscaler location settings configuration (config-zscaler-location-settings) mode. To disable Zscaler custom datacenters, use the **no** form of this command.

datacenters primary-data-center *primary-data-center1*

no datacenters primary-data-center *primary-data-center1*

Syntax Description

primary-data-center *primary-data-center1*	Configures primary data center. Only this option is qualified for use in Cisco SD-WAN Manager CLI templates.

Command Default

Command Modes

zscaler location settings configuration (config-zscaler-location-settings)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

The following example shows how to custom primary data center:

```
Device(config)# sdwan

Device(config-sdwan)# service sig vrf global
Device(config-vrf-global)# zscaler-location-settings
Device(config-zscaler-location-settings)# datacenters
Device(config-zscaler-location-settings)# datacenters primary-data-center
vie1-vpn.zscalerthree.net
```

ips-control

To configure the Zscaler intrusion prevention service (IPS), use the **ips-control** command in zscaler location settings configuration (config-zscaler-location-settings) mode.

ips-control false

Syntax Description

false	Only this option is qualified for use.

Command Default

false

Command Modes

zscaler location settings configuration (config-zscaler-location-settings)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

```
Device(config)# sdwan

Device(config-sdwan)# service sig vrf global
Device(config-vrf-global)# zscaler-location-settings
Device(config-zscaler-location-settings)# ips-control false
```

ofw-enabled

To enable or disable the firewall for a Zscaler location, use the **ofw-enabled** command in Zscaler location settings configuration mode. To disable the firewall for a Zscaler location, use the **no** form of this command.

ofw-enabled false
no ofw-enabled

Syntax Description

false	Disables the firewall for each location. Only this option is qualified for use in Cisco SD-WAN Manager CLI templates.

Command Default

This command is enabled by default.

Command Modes

zscaler location settings configuration (config-zscaler-location-settings)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Security Configuration Guide.

Examples

The following example shows how to disable the firewall for a location:

```
Device (config)# sdwan
Device (config-sdwan)# service sig vrf global
Device (config-sdwan-vrf-global)# zscaler-location-settings
Device (config-zscaler-location-settings)# ofw-enabled false
```

secure-internet-gateway

To configure secure internet gateway, use the **secure-internet-gateway** command in SD-WAN configuration (config-sdwan) mode.

secure-internet-gateway zscaler { **organization** | **partner-base-uri** | **partner-key** | **password** | **username** }

organization	Organization
partner-base-uri	Base URI to be used for the APIs
partner-key	Partner API Key to authenticate with API gateway
password	Password of Zscaler partner account
username	Username of Zscaler partner account

Command Default

Command Modes

SD-WAN configuration (config-sdwan)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

The following example shows how to configure location settings mode:

```
Device(config)# sdwan

Device(config-sdwan)# secure-internet-gateway
Device(config-secure-internet-gateway)# zscaler organization cisco-dev.com
Device(config-secure-internet-gateway)#zscaler partner-base-uri admin.zscalerthree.net/api/v1
Device(config-secure-internet-gateway)#zscaler partner-key SAGv4U2lwh9R
Device(config-secure-internet-gateway)#zscaler username sig-dev@cisco-dev.com
Device(config-secure-internet-gateway)#zscaler password
$8$O0i/6etiDQSqcm+B4yetJDPaYBx1x0wQujnz3pqQG7s=
```

ssl-scan-enabled

To configure Zscaler Secure Sockets Layer (SSL) protocol scan to protect HTTP traffic, use the **ssl-scan** command in zscaler location settings configuration (config-zscaler-location-settings) mode. To disable this command, use the **no** form of this command.

ssl-scan-enabled false

no ssl-scan-enabled

Syntax Description

false	Disables the SSL scan in location settings. Only this option is qualified for use in Cisco SD-WAN Manager CLI templates.

Command Default

This command is disabled by default.

Command Modes

zscaler location settings configuration (config-zscaler-location-settings)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

The following example shows how to disable SSL scan:

```
Device(config)# sdwan

Device(config-sdwan)# service sig vrf global
Device(config-vrf-global)# zscaler-location-settings
Device(config-zscaler-location-settings)# ssl-scan-enabled false
```

surrogate display-time-unit

To display the duration for which the Zscaler service maps a private IP address to a user, use the **surrogate display-time-unit** command in Zscaler location settings configuration mode. To restore the default value, use the **no** form of this command.

surrogate display-time-unit [**DAY** | **HOUR** | **MINUTE**]
no surrogate display-time-unit

Syntax Description

DAY	(Optional) Displays the number of days of mapping between a private IP address and a user.
HOUR	(Optional) Displays the number of hours of mapping between a private IP address and a user.
MINUTES	(Optional) Displays the number of minutes of mapping between a private IP address and a user.

Command Default

The default display time unit is 60 seconds.

Command Modes

zscaler location settings configuration (config-zscaler-location-settings)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Security Configuration Guide.

Examples

The following example shows how to configure the duration in minutes for which the Zscaler service maps a private IP address to a user:

```
Device (config)# sdwan
Device (config-sdwan)# service sig vrf global
Device (config-sdwan-vrf-global)# zscaler-location-settings
Device (config-zscaler-location-settings)# surrogate display-time-unit MINUTE
```

surrogate idle-time

To specify how long after a completed transaction, the Zscaler service mapping to a private IP address of a user is retained, use the **surrogate idle-time** command in Zscaler location settings configuration mode. To remove the Zscaler service mapping to a private IP address of a user, use the **no** form of this command.

surrogate idle-time *idle-time*
no surrogate idle-time

Syntax Description

idle-time	Specifies the time in minutes until which the Zscaler service mapping between the private IP address and a user is retained. Range: 0–4294967295

Command Default

Disabled; no default number is specified.

Command Modes

zscaler location settings configuration (config-zscaler-location-settings)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Security Configuration Guide.

Examples

The following example specifies the time until which the Zscaler service mapping between the private IP address and a user is retained:

```
Device (config)# sdwan
Device (config-sdwan)# service sig vrf global
Device (config-sdwan-vrf-global)# zscaler-location-settings
Device (config-zscaler-location-settings)# surrogate idle-time 43
```

surrogate ip

To enable the Zscaler service to map a user to a private IP address so that it can apply the user's policies, use the **surrogate ip** command in Zscaler location settings configuration mode. To disable the Zscaler service to map to a private IP address, use the **no** form of this command.

surrogate ip false
no surrogate ip

Syntax Description

false	Disables the mapping of a user to a device IP address. Only this option is qualified for use in Cisco SD-WAN Manager CLI templates.

Command Default

By default, this command is set to false.

Command Modes

zscaler location settings configuration (config-zscaler-location-settings)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Security Configuration Guide.

Examples

The following example shows how to disable surrogate ip:

```
Device (config)# sdwan
Device (config-sdwan)# service sig vrf global
Device (config-sdwan-vrf-global)# zscaler-location-settings
Device (config-zscaler-location-settings)# surrogate ip false
```

surrogate ip-enforced-for-known-browsers

To use the existing mapping between IP address and user (acquired from surrogate IP) to authenticate users sending traffic from known browsers, use the **surrogate ip-enforced-for-known-browsers** command in Zscaler location settings configuration mode. To disable the user authentication from known browsers, use the **no** form of this command.

surrogate ip-enforced-for-known-browsers false
no surrogate ip-enforced-for-known-browsers

Syntax Description

false	Disables the Zscaler service to authenticate users on browsers with cookies or other configured authentication mechanisms. Only this option is qualified for use in Cisco SD-WAN Manager CLI templates.

Command Default

This command is enabled by default.

Command Modes

zscaler location settings configuration (config-zscaler-location-settings)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Security Configuration Guide.

Examples

The following example shows how to disable authenticating users who send traffic from known browsers:

```
Device (config)# sdwan
Device (config-sdwan)# service sig vrf global
Device (config-sdwan-vrf-global)# zscaler-location-settings
Device (config-zscaler-location-settings)# surrogate ip-enforced-for-known-browsers false
```

surrogate refresh-time

To configure the length of time that the Zscaler service can use to map between IP address and user, use the **surrogate refresh-time** command in Zscaler location settings configuration mode. To remove the refresh time for revalidation of surrogacy, use the **no** form of this command.

surrogate refresh-time *refresh-time*
no surrogate refresh-time

Syntax Description

refresh-time	Specifies the length of time that the Zscaler service can use to map between IP address and user for authenticating users who sends traffic from known browsers. Range: 0–4294967295 **Note** We recommend that you set the refresh time to a time period shorter than that you specified for the idle time to disassociation.

Command Default

This command is disabled by default.

Command Modes

zscaler location settings configuration (config-zscaler-location-settings)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Security Configuration Guide.

Examples

The following example specifies the length of time that the Zscaler service can use to map between IP address and user:

```
Device (config)# sdwan
Device (config-sdwan)# service sig vrf global
Device (config-sdwan-vrf-global)# zscaler-location-settings
Device (config-zscaler-location-settings)# surrogate refresh-time 0
```

surrogate refresh-time-unit

To view the duration of time that the Zscaler service takes to map IP address to a user, use the **surrogate refresh-time-unit** command in Zscaler location settings configuration mode. To restore the default display of time, use the **no** form of this command.

surrogate refresh-time-unit [**DAY** | **HOUR** | **MINUTE**]
no surrogate refresh-time-unit

Syntax Description

DAY	Displays number of days of mapping between a private IP address and a user for authenticating users who send traffic from a known browser.
HOUR	Displays the number of hours of mapping between a private IP address and a user for authenticating users who send traffic from a known browser.
MINUTES	(Optional) Displays the number of minutes of mapping between a private IP address and a user for authenticating users who send traffic from a known browser.

Command Default

Disabled; no default value is specified.

Command Modes

zscaler location settings configuration (config-zscaler-location-settings)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Security Configuration Guide.

Examples

The following example shows how to display the duration in minutes for which the Zscaler service maps a private IP address to a user who sends traffic from a known browser:

```
Device (config)# sdwan
Device (config-sdwan)# service sig vrf global
Device (config-sdwan-vrf-global)# zscaler-location-settings
Device (config-zscaler-location-settings)# surrogate refresh-time-unit MINUTE
```

tunnel-options

To configure tunnel options, use the **tunnel-options** command in interface tunnel configuration (config-interface-tunnel1) mode.

tunnel-options tunnel-set secure-internet-gateway-zscaler tunnel-dc-preference { **primary-dc** | **secondary-dc** } **source-interface interface-name** *number*

tunnel-options	Tunnel interface configuration
tunnel-set	Tunnel mapping to application type
secure-internet-gateway-zscaler	Tunnel to secure-internet-gateway zscaler
tunnel-dc-preference	Tunnel setup preference to data-center
primary-dc	Tunnel setup to primary data-center
secondary-dc	Tunnel setup to secondary data-center
source-interface	Tunnel source interface

Command Default None.

Command Modes Interface Tunnel configuration (config-interface-tunnel1)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines The following example shows how to configure location settings mode:

```
Device(config)# sdwan
Device(config-sdwan)# interface Tunnel1

Device(config-interface-Tunnel1)# tunnel-options tunnel-set secure-internet-gateway-zscaler
 tunnel-dc-preference primary-dc source-interface GigabitEthernet1
```

xff-forward-enabled

To configure Zscaler X-Forwarded-For (XFF) header in the HTTP to forward traffic, use the **xff-forward** command in zscaler location settings configuration (config-zscaler-location-settings) mode. To disable this command, use the **no** form of this command.

xff-forward-enabled false

no xff-forward-enabled false

Syntax Description

false	Disables the XFF forward HTTP header in location settings. Only this option is qualified for use in Cisco SD-WAN Manager CLI templates.

Command Default This command is disabled by default.

Command Modes zscaler location settings configuration (config-zscaler-location-settings)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines The following example shows how to disable xff-forward:

```
Device(config)# sdwan

Device(config-sdwan)# service sig vrf global
Device(config-vrf-global)# zscaler-location-settings
Device(config-zscaler-location-settings)# xff-forward-enabled false
```

zscaler-location-settings

To configure Zscaler location settings, use the **zscaler-location-settings** command in zscaler location settings configuration (config-zscaler-location-settings) mode.

zscaler-location-settings

This command has no keywords or arguments.

Command Default

Command Modes

zscaler location settings configuration (config-zscaler-location-settings)

Command History

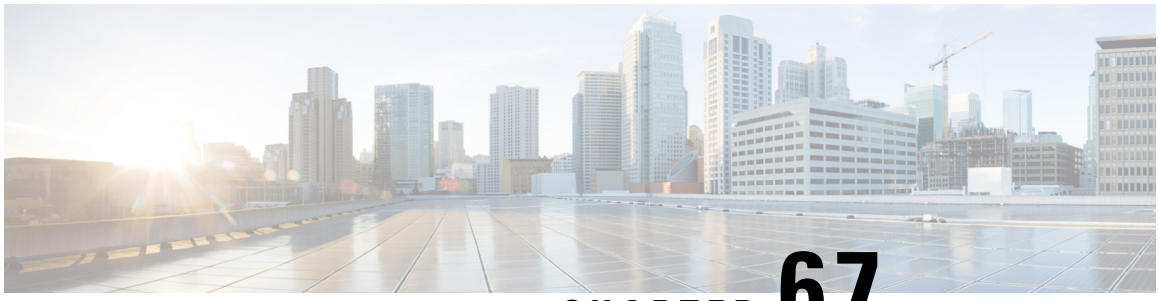
Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

The following example shows how to configure location settings mode:

```
Device(config)# sdwan

Device(config-sdwan)# service sig vrf global
Device(config-vrf-global)# zscaler-location-settings
```



CHAPTER 67

Troubleshooting Commands

- clear ip nat statistics, on page 992
- clear sdwan app-fwd cflowd flow-all, on page 993
- clear sdwan app-fwd cflowd statistics, on page 993
- clear sdwan app-route statistics, on page 994
- clear sdwan appqoe dreopt, on page 995
- clear sdwan bfd transitions, on page 995
- clear sdwan control connection-history, on page 996
- clear sdwan control connections , on page 997
- clear sdwan control port-index, on page 998
- clear sdwan dns app-fwd cflowd flow-all, on page 998
- clear sdwan dns app-fwd cflowd statistics, on page 999
- clear sdwan dns app-fwd dpi flow-all, on page 1000
- clear sdwan dns app-fwd dpi summary, on page 1000
- clear sdwan dns app-route statistics, on page 1001
- clear sdwan dns cache , on page 1001
- clear sdwan installed-certificates, on page 1002
- clear sdwan notification stream viptela, on page 1003
- clear sdwan omp, on page 1003
- clear sdwan policy, on page 1004
- clear sdwan reverse-proxy context, on page 1005
- clear sdwan tunnel gre-keepalive, on page 1006
- clear sdwan tunnel statistics, on page 1007
- clear sdwan umbrella dp-stats, on page 1007
- clear sdwan utd engine standard logging events, on page 1008
- clear sdwan utd engine standard statistics daq vrf, on page 1008
- clear sdwan utd engine standard statistics url-filtering vrf, on page 1009
- clear sdwan utd statistics, on page 1010
- clear sdwan zbfw statistics drop, on page 1011
- debug packet-trace condition, on page 1012
- debug platform condition match, on page 1013
- debug platform condition start, on page 1014
- debug platform condition stop, on page 1014
- debug platform condition feature sdwan controlplane bfd, on page 1015

- debug platform software sdwan fpm, on page 1015
- debug vdaemon, on page 1016
- debug platform software sdwan vdaemon , on page 1018
- set platform software trace, on page 1019
- set platform software trace vdaemon, on page 1020
- show sdwan control connections, on page 1021
- monitor capture (access list/class map), on page 1022
- monitor capture (interface/control plane), on page 1024
- monitor capture match ipv4, on page 1025
- monitor capture match ipv6, on page 1025
- privilege exec level, on page 1027
- request nms sdavc-gw, on page 1028
- request nms patch all, on page 1029
- request nms unpatch, on page 1031
- request nms container-manager diagnostics, on page 1032
- request platform software sdwan admin-tech, on page 1035
- request platform software sdwan auto-suspend reset, on page 1036
- request platform software sdwan certificate install , on page 1037
- request platform software sdwan config reset , on page 1038
- request platform software sdwan csr upload, on page 1039
- request platform software sdwan port_hop color, on page 1040
- request platform software sdwan root-cert-chain install, on page 1041
- request platform software sdwan root-cert-chain uninstall, on page 1042
- request platform software sdwan software activate , on page 1042
- request platform software sdwan software install, on page 1043
- request platform software sdwan software remove, on page 1044
- request platform software sdwan software secure-boot , on page 1045
- request platform software sdwan software set-default, on page 1045
- request platform software sdwan software upgrade-confirm , on page 1046
- set platform software trace, on page 1047
- show platform software sdwan interface-alarm summary , on page 1055
- show aaa servers, on page 1056
- show autoip status, on page 1056
- show class map type inspect, on page 1057
- show cellular, on page 1058
- show clock, on page 1059
- show config-pull history, on page 1060
- Show config-pull transactions, on page 1061
- show configuration commit list, on page 1066
- show crypto ipsec sa, on page 1067
- show cts environment-data, on page 1072
- show cts pac, on page 1073
- show cts role-based counters, on page 1074
- show cts role-based permissions, on page 1075
- show cts role-based sgt-map, on page 1076
- show cts sxp connections, on page 1077

- show crypto key mypubkey rsa, on page 1079
- show crypto ikev2 stats, on page 1080
- show crypto pki certificates, on page 1081
- show crypto session, on page 1084
- show endpoint-tracker, on page 1085
- show etherchannel load-balancing, on page 1089
- show etherchannel summary, on page 1089
- show flow exporter, on page 1090
- show flow monitor sdwan_flow_monitor cache, on page 1097
- show flow record, on page 1098
- show full-configuration probe-path load-balance-dia, on page 1099
- show geo file-contents info, on page 1100
- show geo status, on page 1100
- show interfaces, on page 1101
- show interface port-channel, on page 1105
- show interface port-channel etherchannel, on page 1107
- show inventory, on page 1108
- show idmgr status, on page 1110
- show idmgr omp ip-user-bindings, on page 1111
- show idmgr omp user-usergroup-bindings, on page 1111
- show idmgr user-sessions, on page 1112
- show ip bgp ipv4, on page 1113
- show ip bgp vpnv4, on page 1115
- show ip bgp vpnv4 vrf, on page 1124
- show ip dhcp binding, on page 1125
- show ip cef vrf, on page 1126
- show ip msdp vrf count, on page 1127
- show ip msdp vrf peer, on page 1127
- show ip msdp vrf sa-cache, on page 1128
- show ip msdp vrf summary, on page 1129
- show ip interface, on page 1129
- show ip interface brief, on page 1132
- show ip nat redundancy, on page 1133
- show ip nat route-dia, on page 1134
- show ip nat statistics, on page 1134
- show ip nat translations, on page 1136
- show ip nat status, on page 1139
- show running nat, on page 1140
- show ip pim bsr-router, on page 1141
- show ip pim rp, on page 1141
- show ip protocols, on page 1142
- show ip rip database, on page 1145
- show ip rip neighbors, on page 1146
- show ip route, on page 1147
- show ip route rip, on page 1157
- show ip route vrf, on page 1158

- show ip sla summary, on page 1162
- show ipv6 access-list, on page 1163
- show ipv6 dhcp binding, on page 1163
- show ipv6 dhcp database, on page 1164
- show ipv6 dhcp interface, on page 1165
- show ipv6 dhcp pool, on page 1166
- show ipv6 route vrf, on page 1167
- show key chain, on page 1168
- show lacp, on page 1168
- show lte450 all, on page 1170
- show lte450 network, on page 1172
- show lte450 hardware, on page 1173
- show lte450 radio, on page 1174
- show logging cacert, on page 1175
- show logging profile sdwan internal filter , on page 1175
- show macsec hw detail, on page 1177
- show macsec mka-request-notify, on page 1178
- show macsec summary, on page 1178
- show macsec status interface, on page 1179
- show mka default-policy, on page 1180
- show mka keychains, on page 1183
- show mka policy, on page 1183
- show mka sessions, on page 1184
- show mka statistics, on page 1187
- show mka summary, on page 1187
- show nat66 dia route, on page 1189
- show nat64 map-e, on page 1190
- show nat66 nd, on page 1190
- show nat66 prefix, on page 1191
- show nat66 statistics, on page 1192
- show object-group, on page 1192
- show policy-firewall session platform detail, on page 1193
- show performance monitor cache, on page 1194
- show performance monitor context, on page 1195
- show platform hardware qfp active classification class-group-manager class-group client cce name, on page 1199
- show platform hardware qfp active classification class-group-manager class-group client sdwan, on page 1200
- show platform hardware qfp active classification class-group-manager object-group, on page 1201
- show platform hardware qfp active classification feature message all, on page 1203
- show platform hardware qfp active classification feature-manager exmem-usage, on page 1204
- show platform hardware qfp active classification feature-manager statistics, on page 1205
- show platform hardware qfp active feature acl control, on page 1206
- show platform hardware qfp active feature acl dp hsl configuration, on page 1208
- show platform hardware qfp active feature acl dp hsl statistics, on page 1210
- show platform hardware qfp active feature bfd datapath, on page 1211

- show platform hardware qfp active feature bfd datapath, on page 1213
- show platform hardware qfp active feature firewall drop, on page 1215
- show platform hardware qfp active feature geo client, on page 1216
- show platform hardware qfp active feature geo datapath, on page 1217
- show platform hardware qfp active feature nat datapath hsl, on page 1218
- show platform hardware qfp active feature nat datapath map, on page 1219
- show platform hardware qfp active feature nat datapath sess-dump, on page 1220
- show platform hardware qfp active feature nat datapath stats, on page 1221
- show platform hardware qfp active feature nat datapath summary, on page 1221
- show platform hardware qfp active feature nat66 datapath prefix, on page 1223
- show platform hardware qfp active feature nat66 datapath statistics, on page 1224
- show platform hardware qfp active feature sdwan client phy-wan-bind-list, on page 1224
- show platform hardware qfp active feature utd config, on page 1225
- show platform hardware qfp active interface if-name, on page 1226
- show platform hardware qfp active statistics drop, on page 1227
- show platform hardware qfp active feature firewall datapath rg, on page 1228
- show platform hardware qfp active feature firewall drop all, on page 1231
- show platform hardware qfp active feature bridge-domain datapath sdwan-flood-list, on page 1233
- show platform packet-trace, on page 1234
- show platform packet-trace fia-statistics, on page 1236
- show platform software common-classification f0 tag, on page 1237
- show platform software cpu alloc, on page 1239
- show platform software ipsec fp active flow , on page 1241
- show platform software ipsec ftm-msg-stats, on page 1245
- show platform software ipsec sdwanrp-msg-stats, on page 1246
- show platform software ipsec vesen-event-log, on page 1247
- show platform software memory, on page 1248
- show platform software nat66 fp active, on page 1250
- show platform software nat66 rp active, on page 1251
- show platform software sdwan ftmd bridge-domain, on page 1252
- show platform software sdwan multicast active-sources vrf, on page 1253
- show platform software sdwan multicast remote-nodes vrf, on page 1253
- show platform software sdwan qos , on page 1254
- show platform software sdwan tloc-db, on page 1256
- show platform software sdwan ttmd local-tlocs, on page 1257
- show platform software sdwan ttmd history tloc, on page 1258
- show platform software sdwan ttmd tlocs stats, on page 1259
- show policy-firewall config, on page 1259
- show policy-map interface Port-channel, on page 1260
- show processes cpu platform, on page 1262
- show policy-map type inspect, on page 1264
- show power, on page 1264
- show raw-socket, on page 1266
- show redundancy application control-interface group, on page 1267
- show redundancy application data-interface group, on page 1268
- show redundancy application group, on page 1269

- show redundancy application group protocol, on page 1272
- show redundancy rii, on page 1273
- show sd-routing certificate staged, on page 1274
- show sdwan alarms detail, on page 1275
- show sdwan alarms summary, on page 1276
- show sdwan appqoe, on page 1277
- show sdwan appqoe dreopt, on page 1281
- show sdwan appqoe dreopt statistics, on page 1283
- show sdwan appqoe error recent, on page 1284
- show sdwan appqoe flow closed all, on page 1288
- show sdwan appqoe flow closed flow-id, on page 1289
- show sdwan appqoe flow flow-id, on page 1294
- show sdwan appqoe flow vpn-id, on page 1299
- show sdwan appqoe status, on page 1300
- show sdwan app-fwd cflowd collector, on page 1301
- show sdwan app-fwd cflowd flows, on page 1302
- show sdwan app-fwd cflowd flow-count, on page 1304
- show sdwan app-fwd cflowd statistics, on page 1305
- show sdwan app-fwd cflowd template, on page 1306
- show sdwan app-fwd dpi flows, on page 1307
- show sdwan app-fwd dpi summary, on page 1310
- show sdwan app-route sla-class, on page 1311
- show sdwan app-route stats, on page 1312
- show sdwan bfd history, on page 1316
- show sdwan bfd sessions, on page 1317
- show sdwan bfd sessions region-access, on page 1319
- show sdwan bfd sessions region-core, on page 1320
- show sdwan bfd summary, on page 1320
- show sdwan bfd tloc-summary-list, on page 1322
- show sdwan certificate, on page 1323
- show sdwan certificate staged, on page 1328
- show sdwan cloudexpress applications, on page 1329
- show sdwan cloudexpress gateway-exits, on page 1331
- show sdwan cloudexpress load-balance applications, on page 1333
- show sdwan cloudexpress local-exits, on page 1335
- show sdwan control, on page 1336
- show sdwan debugs, on page 1342
- show sdwan firmware-packages details, on page 1344
- show sdwan firmware-packages list, on page 1344
- show sdwan from-vsmart commit-history, on page 1345
- show sdwan from-vsmart policy, on page 1347
- show sdwan from-vsmart tag-instances, on page 1349
- show sdwan ftm umts, on page 1350
- show sdwan ftm umts logs, on page 1351
- show sdwan geofence-status, on page 1352
- show sdwan interface color, on page 1353

- show sdwan ipsec inbound-connections, on page 1353
- show sdwan ipsec local-sa, on page 1355
- show sdwan ipsec outbound-connections, on page 1356
- show sdwan ipsec pwk inbound-connections, on page 1357
- show sdwan ipsec pwk local-sa, on page 1359
- show sdwan ipsec pwk outbound-connections, on page 1360
- show sdwan nat-fwd ip-nat-translation, on page 1362
- show sdwan nat-fwd ip-nat-translation-verbose, on page 1363
- show sdwan omp cloudexpress, on page 1364
- show sdwan omp ipv6-routes, on page 1366
- show sdwan omp multicast-auto-discover, on page 1368
- show sdwan omp multicast-routes, on page 1369
- show sdwan omp peers, on page 1370
- show sdwan omp routes, on page 1374
- show sdwan omp l2-routes, on page 1379
- show sdwan omp services, on page 1385
- show sdwan omp summary, on page 1386
- show sdwan omp tlocs, on page 1389
- show sdwan policy access-list-associations, on page 1396
- show sdwan policy access-list-counters, on page 1397
- show sdwan policy access-list-names, on page 1397
- show sdwan policy access-list-policers, on page 1398
- show sdwan policy app-route-policy-filter, on page 1398
- show sdwan policy data-policy-filter, on page 1400
- show sdwan policy from-vsmart, on page 1402
- show sdwan policy ipv6 access-list-associations, on page 1403
- show sdwan policy ipv6 access-list-counters, on page 1404
- show sdwan policy ipv6 access-list-names, on page 1405
- show sdwan policy ipv6 access-list-policers, on page 1405
- show sdwan policy rewrite-associations, on page 1406
- show sdwan reboot history, on page 1407
- show sdwan running-config, on page 1408
- show sdwan security-info, on page 1411
- show sdwan secure-internet-gateway tunnels, on page 1411
- show sdwan secure-internet-gateway umbrella tunnels, on page 1413
- show sdwan secure-internet-gateway zscaler tunnels, on page 1414
- show sdwan software, on page 1415
- show platform software sdwan dta cflowd statistics , on page 1416
- show sdwan system status, on page 1417
- show sdwan tag-instances from-vsmart, on page 1420
- show sdwan version, on page 1421
- show sdwan zbfw drop-statistics, on page 1421
- show sdwan zbfw zonepair-statistics, on page 1423
- show sdwan zonebfwdp sessions, on page 1424
- show service-insertion type appqoe, on page 1426
- show sslproxy statistics, on page 1428

- show sslproxy status, on page 1429
- show standby, on page 1431
- show standby neighbors, on page 1435
- show support policy route-policy, on page 1437
- show tech-support sdwan bfd, on page 1438
- show track, on page 1442
- show uidp statistics, on page 1444
- show uidp user-group all, on page 1445
- show uidp user ip, on page 1446
- show utd engine standard config, on page 1446
- show utd unified-policy, on page 1448
- show vrrp, on page 1449
- show wireless-bridge status, on page 1452
- show wireless-lan radio, on page 1453
- show wireless-lan wlan, on page 1453
- show wireless-lan client, on page 1454
- show zone-pair security, on page 1455
- verify, on page 1455
- vdiagnose vmanage cluster, on page 1456

clear ip nat statistics

To clear the NAT datapath map and session information, use the **clear ip nat statistics** command in privileged EXEC mode.

clear ip nat statistics

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	This command is supported for Cisco Catalyst SD-WAN.

Usage Guidelines

Use the **ip nat clear statistics** command to clear the NAT datapath map and session information.

Examples

The following is a sample output from the **ip nat clear statistics** command:

```
Device# ip nat clear statistics
```

clear sdwan app-fwd cflowd flow-all

To clear the cflowd flows in all VPNs, use the **clear sdwan app-fwd cflowd flow-all** command in privileged exec mode.

clear sdwan app-fwd cflowd flow-all

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Privileged exec (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines This command can be used to clear all the cflowd flows from all VPNs in a Cisco IOS XE Catalyst SD-WAN device.

Example

The following example shows how to clear the cflowd flows from all VPNs from a Cisco IOS XE Catalyst SD-WAN device.

```
Device# clear sdwan app-fwd cflowd flow-all
```

Related Commands

Command	Description
clear sdwan app-fwd cflowd statistics	Clears all cflowd statistics from a Cisco IOS XE Catalyst SD-WAN device.

clear sdwan app-fwd cflowd statistics

To clear the cflowd packet statistics, use the **clear sdwan app-fwd cflowd statistics** command in privileged EXEC mode.

clear sdwan app-fwd cflowd statistics

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

This command can be used to clear the cflowd packet statistics from a Cisco IOS XE Catalyst SD-WAN device.

Example

The following example shows how to clear the cflowd packet statistics from a Cisco IOS XE Catalyst SD-WAN device.

```
Device# clear sdwan app-fwd cflowd statistics
```

Related Commands

Command	Description
clear sdwan app-fwd cflowd flow-all	Clears all cflowd flows from a Cisco IOS XE Catalyst SD-WAN device.

clear sdwan app-route statistics

To clear the app-route statistics from a Cisco IOS XE Catalyst SD-WAN device, use the **clear sdwan app-route statistics** command in privileged EXEC mode.

clear sdwan app-route statistics

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

This command can be used to clear the application aware routing statistics from a Cisco IOS XE Catalyst SD-WAN device.

Example

The following example shows how to clear the app-route statistics from a Cisco IOS XE Catalyst SD-WAN device.

```
Device# clear sdwan app-route statistics
```

clear sdwan appqoe dreopt

To clear DRE cache and restart DRE service, use the **clear sdwan appqoe dreopt cache** command in privileged EXEC mode.

clear sdwan appqoe dreopt { **cache** | **statistics** [**peer**] [**peer-no** *peer-id*] | **auto-bypass** [**server** *server-ip server-port*] }

Syntax Description

cache	Clears DREOPT cache.
statistics	Clears global DRE statistics.
peer	(Optional) Clears DREOPT peer statistics table.
peer-no *peer-id*	(Optional) Clears DREOPT statistics using peer-no for the specified peer ID.
auto-bypass	Clears DRE auto-bypass table.
server *server-ipserver-port*	Clears DRE auto-bypass entries for the specified server IP address and server port.

Command Default

This command has no default behavior.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	This command can be used in SD-WAN controller mode.

Example

The following example shows how to clear DRE cache.

```
Device# clear sdwan appqoe dreopt cache

DRE cache successfully cleared
```

clear sdwan bfd transitions

To clear all Bidirectional Forwarding Detection (BFD) transition counters from a Cisco IOS XE Catalyst SD-WAN device, use the **clear sdwan bfd transitions** command in privileged EXEC mode.

clear sdwan bfd transitions

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templ

Usage Guidelines The BFD protocol detects link failures as part of the Cisco SD-WAN high availability solution and by default, it is enabled on all Cisco IOS XE Catalyst SD-WAN devices. You cannot disable this protocol. The BFD protocol functionalities include path liveliness and quality measurement.

This command is used to clear all BFD transitions counters from a Cisco IOS XE Catalyst SD-WAN device.

Example

The following example clears all BFD transition counters from a Cisco IOS XE Catalyst SD-WAN device.

```
Device# clear sdwan bfd transitions
```

Related Commands

Command	Description
show sdwan bfd sessions	Displays information about the BFD sessions.
show sdwan bfd history	Displays the history of the BFD sessions.

clear sdwan control connection-history

To erase the connection history on a Cisco IOS XE Catalyst SD-WAN device, use the **clear sdwan control connection-history** command in privileged EXEC mode.

clear sdwan control connection-history

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines Cisco IOS XE SD-WAN devices establish control plane connection with Cisco SD-WAN Controllers (Cisco SD-WAN Manager, Cisco Catalyst SD-WAN Controller, and Cisco Catalyst SD-WAN Validator), and maintains these connections with Cisco Catalyst SD-WAN Controller and Cisco SD-WAN Manager.

This command can be used to erase all the connection history information from the Cisco IOS XE Catalyst SD-WAN devices.

Example

The following example erases the connection history information from a Cisco IOS XE Catalyst SD-WAN device:

```
Device# clear sdwan control connections-history
```

Related Commands

Command	Description
clear control connections	Resets the DTLS connections from a local device to all Cisco IOS XE Catalyst SD-WAN devices.
show sdwan control connection-history	Displays control connection history.

clear sdwan control connections

To reset the DTLS connections from a Cisco IOS XE Catalyst SD-WAN device to the SD-WAN controllers, use the **clear sdwan control connections** command in privileged EXEC mode.

clear sdwan control connections

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines Cisco IOS XE SD-WAN devices establish control plane connection with Cisco SD-WAN Controllers (Cisco SD-WAN Manager, Cisco Catalyst SD-WAN Controller, and Cisco Catalyst SD-WAN Validator), and maintains these connections with Cisco Catalyst SD-WAN Controller and Cisco SD-WAN Manager.

This command can be used to reset the DTLS connections from a Cisco IOS XE Catalyst SD-WAN device to the Cisco SD-WAN Controllers.

Example

The following example shows how to reset the DTLS connections.

```
Device# clear sdwan control connections
```

Related Commands

Command	Description
clear control connections-history	Erases the connection history on a Cisco IOS XE Catalyst SD-WAN device.

Command	Description
show sdwan control connections	Displays information about control connections.
show sdwan control connection-history	Displays information about control connections history.

clear sdwan control port-index

To reset port-hop back to the base port on Cisco IOS XE Catalyst SD-WAN devices, use the **clear sdwan control port-index** command in privileged EXEC mode.

clear sdwan control port-index

Syntax Description This command has no keywords or arguments.

Command Default This command has no default behavior.

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	This command was introduced.

Usage Guidelines Use the **clear sdwan control port-index** command to reach back to 12346 base port on all the WAN interfaces.

Examples

The following example shows how to clear SD-WAN control port-index:

```
Device# clear sdwan control port-index
```

clear sdwan dns app-fwd cflowd flow-all

To clear the DNS cache for all cflowd flows, use the **clear sdwan dns app-fwd cflowd flow-all** command in privileged EXEC mode.

clear sdwan dns app-fwd cflowd flow-all

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines This command can be used to clear the DNS cache for all cflowd flows in a Cisco IOS XE Catalyst SD-WAN device.

Example

The following example shows how to clear the DNS cache for all cflowd flows in a Cisco IOS XE Catalyst SD-WAN device.

```
Device# clear sdwan dns app-fwd cflowd flow-all
```

Related Commands

Command	Description
clear control connections-history	Erases the connection history on a Cisco IOS XE Catalyst SD-WAN device.
clear sdwan dns app-fwd cflowd flow-all	Clears all cflowd flows.

clear sdwan dns app-fwd cflowd statistics

To clear the cflowd statistics from a Cisco IOS XE Catalyst SD-WAN device, use the **clear sdwan dns app-fwd cflowd statistics** command in privileged EXEC mode.

clear sdwan dns app-fwd cflowd statistics

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI te

Usage Guidelines This command can be used to clear the cflowd statistics from a Cisco IOS XE Catalyst SD-WAN device.

Example

The following example shows how to clear the cflowd statistics from a Cisco IOS XE Catalyst SD-WAN device.

```
Device# clear sdwan dns app-fwd cflowd statistics
```

Related Commands

Command	Description
clear sdwan dns app-fwd cflowd flow-all	Clears all cflowd flows from a Cisco IOS XE Catalyst SD-WAN device.

clear sdwan dns app-fwd dpi flow-all

To clear the DNS Deep Packet Inspection (DPI) flows from a Cisco IOS XE Catalyst SD-WAN device, use the **clear sdwan dns app-fwd dpi flow-all** command in privileged exec mode.

clear sdwan dns app-fwd dpi flow-all

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Privileged exec (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templa

Usage Guidelines

This command can be used to clear the DNS DPI flows from a Cisco IOS XE Catalyst SD-WAN device.

Example

The following example shows how to clear the dpi flows from a Cisco IOS XE Catalyst SD-WAN device.

```
Device# clear sdwan dns app-fwd dpi flow-all
```

Related Commands

Command	Description
clear sdwan dns app-fwd dpi summary	Clears all DPI statistics.

clear sdwan dns app-fwd dpi summary

To clear all known dpi statistics for all related app information, use the **clear sdwan dns app-fwd dpi summary** command in privileged EXEC mode. This command does not have a **no** form.

clear sdwan dns app-fwd dpi summary

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines Use this command to clear out any dpi statistics for all related app information.

Example

The following example clears the dpi statistics for all related app information.

```
Device#clear sdwan dns app-fwd dpi summary
```

Table 71: Related Commands

Commands	Description
clear sdwan dns app-fwd dpi flow-all	Clears all dpi flows in the entire system.

clear sdwan dns app-route statistics

To clear all app-route statistics, use the **clear sdwan dns app-route statistics** command in privileged EXEC mode. This command does not have a **no** form.

clear sdwan dns app-route statistics

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines Use this command to clear all app route related statistics from the system.

Example

The following example clears all app route statistics from the router.

```
Device# clear sdwan dns app-route statistics
```

clear sdwan dns cache

To clear the cache of DNS entries on a Cisco IOS XE Catalyst SD-WAN device, use the **clear sdwan dns cache** command in privileged EXEC mode.

clear sdwan dns cache

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Ma

Usage Guidelines The DNS cache is populated when a Cisco IOS XE Catalyst SD-WAN device establishes a connection with the Cisco Catalyst SD-WAN Validator. For a Cisco IOS XE Catalyst SD-WAN device, this connection is transient, and the DNS cache is cleared when the connection to the Cisco Catalyst SD-WAN Validator is closed.

This command can be used to clear the DNS cache from a Cisco IOS XE Catalyst SD-WAN device.

Example

The following example shows how to clear the DNS cache from a Cisco IOS XE Catalyst SD-WAN device.

```
Device# clear sdwan dns cache
```

Command	Description
show sdwan control local-properties	Displays control plane local properties, including entries in the DNS cache.

clear sdwan installed-certificates

To clear all the installed certificates from a Cisco IOS XE Catalyst SD-WAN device, use the **clear sdwan installed-certificates** command in privileged EXEC mode.

clear sdwan installed-certificates

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines This command can be used to clear all the installed certificates from a Cisco IOS XE Catalyst SD-WAN device, including the public and private keys, and the root certificate. After clearing all certificates from a device, the command resets the device to factory default.

Example

The following example shows how to clear all the installed certificates from a Cisco IOS XE Catalyst SD-WAN device.

```
Device# clear sdwan installed-certificates
```

Related Commands

Command	Description
show sdwan control local-properties	Displays control plane local properties, including entries in the DNS cache.

clear sdwan notification stream viptela

To clear the SD-WAN notification stream viptela, use the **clear sdwan notification stream viptela** command in privileged EXEC mode.

clear sdwan notification stream viptela

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines Use this command to clear the sdwan notification stream viptela.

Example

The following example shows how to clear the sdwan notification stream viptela.

```
Device#clear sdwan notification stream viptela
```

clear sdwan omp

To clear Cisco SD-WAN Overlay Management Protocol (OMP) peers, routes,and TLOCs, use the **clear sdwan omp** command in privileged exec mode.

clear sdwan omp { **all** | **peer** [*ipv4 address*] | **routes** | **tlocs** }

Syntax Description

all	Clears all OMP peering sessions with all OMP peers.

peer	Clears the OMP peering sessions with a specific peer.
ipv4 address	(Optional) Specifies an IPv4 address of the OMP peer.
routes	Clears OMP routes.
tlocs	Clears OMP TLOCs.

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Privileged exec (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

By default, all Cisco IOS XE Catalyst SD-WAN Edge devices establishes OMP peering with Cisco Catalyst SD-WAN Controllers.

This command can be used to clear Cisco SD-WAN OMP peers, routes, and TLOCs that it learns from the Cisco Catalyst SD-WAN Controller.

Example

The following example shows how to reset OMP peering sessions.

```
Device# clear sdwan omp all
```

The following example shows how to clear OMP peering session with a specific peer.

```
Device# clear sdwan omp peer 10.10.10.10
```

The following example shows how to clear OMP routes.

```
Device# clear sdwan omp routes
```

Related Commands

Command	Description
show sdwan omp peers	Displays information about all OMP peering sessions.
show sdwan omp routes	Displays information about OMP routes.
show sdwan omp tlocs	Displays information learned from the TLOC routes advertised using OMP sessions.

clear sdwan policy

To reset counters for IPv6 access lists, route policies, or data policies, use the **clear sdwan policy** command in privileged EXEC mode.

clear sdwan policy { **access-list** [*acl-name*] | **app-route-policy** [*policy-name*] | **ipv6-access-list** [*access-list-name*] | **data-policy** [*policy-name*] }

Syntax Description

acl-name	(Optional) Clears the counters associated with the specified access list.
policy-name	(Optional) Clears the counters associated with the specified application-aware routing policy.
access-list-name	(Optional) Clears Cisco SD-WAN policy IPv6 access-list counters.
policy-name	(Optional) Clears the counters associated with the specified data policy.

Command Default

None

Command Modes

Privileged exec (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manage

Usage Guidelines

The SD-WAN centralized policies comes from the Cisco Catalyst SD-WAN Controller to Cisco IOS XE Catalyst SD-WAN devices.

This command can be used to clear counters for IPv6 access lists, data policies, or route policies.

Example

The following example shows how to clear all access lists.

```
Device# clear sdwan policy access-list
```

The following example shows how to clear all app-route-policy.

```
Device# clear sdwan policy app-route-policy
```

The following example shows how to clear all IPv6 access lists.

```
Device# clear sdwan policy ipv6-access-list
```

Related Commands

Command	Description
show sdwan policy from-vsmart	Displays Cisco SD-WAN centralized policies from Cisco Catalyst SD-WAN Controller.

clear sdwan reverse-proxy context

To clear the signed certificate installed for authentication with a reverse proxy device and reset the control connections to the reverse proxy device, use the **clear sdwan reverse-proxy context** command in privileged EXEC mode.

clear sdwan reverse-proxy context

Syntax Description This command has no keywords or arguments

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 17.6.1a	Command introduced.

Example

```
Device# clear sdwan reverse-proxy context
```

clear sdwan tunnel gre-keepalive

To clear the GRE tunnel keepalives, use the **clear sdwan tunnel gre-keepalive** command in privileged EXEC mode.

clear sdwan tunnel gre-keepalive

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines Use **clear sdwan tunnel gre-keepalive** command to clear the SD-WAN tunnel gre-keepalives.

Example

The following example shows how to clear the SD-WAN tunnel gre keepalives.

```
Device# clear sdwan tunnel gre-keepalive
```

Table 72: Related Commands

Commands	Description
clear sdwan tunnel statistics	Clears SD-WAN tunnel statistics.

clear sdwan tunnel statistics

To reset the information about the packets received on the IPsec connections for the Cisco IOS XE Catalyst SD-WAN devices, use the **clear sdwan tunnel statistics** command in privileged EXEC mode.

clear sdwan tunnel statistics

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines This command can be used to reset the information about the packets transmitted and received on the IPsec connections that originate on Cisco IOS XE Catalyst SD-WAN devices.

Example

The following example shows how to reset the information about the packets transmitted and received on the IPsec connections.

```
Device# clear sdwan tunnel statistics
```

Related Commands

Command	Description
show sdwan tunnel statistics	Displays information about the packets transmitted and received on the IPsec connections.

clear sdwan umbrella dp-stats

To clear the umbrella dp-stats, use the **clear sdwan umbrella dp-stats** command in privileged EXEC mode. This command does not have a **no** form.

clear sdwan umbrella dp-stats

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Use **clear sdwan umbrella dp-stats** command to clear the SD-WAN umbrella datapath stats.

Example

The following example shows how to clear the SD-WAN umbrella data path stats.

```
Device# clear sdwan umbrella dp-stats
```

clear sdwan utd engine standard logging events

To clear SD-WAN UTD engine logging events, use the **clear sdwan utd engine standard logging events** command in privileged EXEC mode.

clear sdwan utd engine standard logging events

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Use **clear sdwan utd engine standard logging events** command to clear the SD-WAN UTD engine logging events.

Example

The following example shows how to clear the SD-WAN UTD engine logging events.

```
Device# clear sdwan utd engine standard logging events
```

clear sdwan utd engine standard statistics daq vrf

To clear SD-WAN UTD engine statistics for all VRFs or a specific VRF, use the **clear sdwan utd engine standard statistics daq vrf** command in privileged EXEC mode. This command does not have a **no** form.

clear sdwan utd engine standard statistics daq vrf { **global** | *name* }

Syntax Description

global	Clears SD-WAN UTD engine standard statistics for all VRFs.
name	Clears SD-WAN UTD engine standard statistics for a specific VRF.

Command Default

None

Command Modes

Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Use this command to clear the SD-WAN UTD engine standard statistics for all VRFs or a specific VRF.

Example

The following example shows how to clear the SD-WAN UTD engine statistics for all VRFs.

```
Device# clear sdwan utd engine standard statistics daq vrf global
```

clear sdwan utd engine standard statistics url-filtering vrf

To clear SD-WAN UTD engine url-filtering statistics all VRFs or for a specific VRF, use the **clear sdwan utd engine standard statistics url-filtering vrf** command in privileged EXEC mode. This command does not have a **no** form.

clear sdwan utd engine standard statistics url-filtering vrf { **global** | *name* }

Syntax Description

global	Clears SD-WAN UTD engine standard statistics for all VRFs.
name	Clears SD-WAN UTD engine standard statistics for a specific VRF.

Command Default

None

Command Modes

Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Use this command to clear the SD-WAN UTD engine standard url-filtering statistics for all VRFs or for a specific VRF.

Example

The following example shows how to clear the SD-WAN UTD engine url filtering statistics for all VRFs.

```
Device# clear sdwan utd engine standard statistics url-filter vrf global
```

clear sdwan utd statistics

To clear SD-WAN UTD statistics, use the **clear sdwan utd statistics** command in privileged EXEC mode. This command does not have a **no** form.

clear sdwan utd statistics { **channel** [*service* | *threat-defense*] | **default** [**channel** | **context** | **policy** | **tls-decrypt** | **vrf**] | **divert** | **drop** | **general** | **policy** [*all*] | **sn** | **summary** | **tls-decrypt** | **vrf** [**default** | **global** | *id* | *name*] }

Syntax Description

channel	Clears channel-specific UTD dataplane statistics.
service	Clears UTD dataplane stats for service channel.
threat-defense	Clears UTD dataplane stats for threat-defense channel.
default	Clears SD-WAN UTD statistics default.
context	Clears SD-WAN UTD statistics default context.
policy	Clears UTD dataplane policy statistics.
tls-decrypt	Clears SD-WAN UTD statistics tls-decrypt.
vrf	Clears SD-WAN UTD statistics VRF.
divert	Clears SD-WAN UTD statistics divert.
drop	Clears SD-WAN UTD statistics drop.
general	Clears SD-WAN UTD statistics general.
policy	Clears UTD dataplane policy statistics.
all	Clears UTD dataplane policy statistics all.
sn	Clears SD-WAN UTD statistics sn.
summary	Clears SD-WAN UTD statistics summary.
vrf	Clears SD-WAN UTD statistics VRF.
default	Clears SD-WAN UTD statistics VRF default.
global	Clears SD-WAN UTD statistics VRF global.
id	Clears SD-WAN UTD statistics VRF ID.

name	Clears SD-WAN UTD statistics VRF name.

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines Use this command to clear SD-WAN UTD statistics.

Example

The following example shows how to clear the SD-WAN UTD statistics from the default VRF.

```
Device# clear sdwan utd statistics vrf default
```

clear sdwan zbfw statistics drop

To clear SD-WAN ZBFW drop statistics, use the **clear sdwan zbfw statistics drop** command in privileged EXEC mode. This command does not have a **no** form.

clear sdwan zbfw statistics drop

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines Use **clear sdwan zbfw statistics drop** command to clear the SD-WAN ZBFW drop statistics.

Example

The following example shows how to clear the SD-WAN ZBFW drop statistics.

```
Device# clear sdwan zbfw statistics drop
```

debug packet-trace condition

To enable packet tracing on edge devices, use the **debug packet-trace condition** command in privileged EXEC mode.

debug packet-trace condition [**start** | **stop**] [**bidirectional**] [**circular**] [**destination-ip** *ip-address*] [**ingress-if** *interface*] [**logging**] [**source-ip** *ip-address*] [**vpn-id** *vpn-id*]

Syntax Description

bidirectional	(Optional) Enables bidirectional flow debugging for source IP and destination IP.
circular	(Optional) Enables circular packet tracing. In this mode, the 1024 packets in the buffer are continuously overwritten.
clear	(Optional) Clears all the debug configurations and packet tracer memory.
destination-ip	(Optional) Specifies the destination IPv4 address.
ingress-if	(Optional) Specifies the ingress interface name. Note: It is must to choose VPN to configure the interface.
logging	(Optional) Enables the packet tracer debug logging.
source-ip	(Optional) Specifies the source IP address.
start	(Optional) Starts the conditional debugging.
stop	(Optional) Stops the conditional debugging.
vpn-id	(Optional) Enables the packet tracing for the specified VPN.

Command Default

None

Command Modes

Privileged EXEC (#)

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	This command was introduced.

Usage Guidelines

The parameters after the keywords **start** and **stop** can be configured in any order.

Example

The following example shows how to configure conditions for packet tracing:

```
Device# debug packet-trace condition source-ip 10.0.0.1
Device# debug packet-trace condition vpn-id 0
Device# debug packet-trace condition interface ge0/1
Device# debug packet-trace condition stop
```

debug platform condition match

To filter IPv4 and IPv6 debugging output for certain **debug** commands on the basis of specified conditions, use the **debug platform condition match protocol** command in privileged EXEC mode. To remove the specified condition, use the **no** form of this command.

debug platform condition interface *interface name* **match** [{ **ipv4 | ipv6** }] **protocol** [{ **tcp** | **udp** | **protocol_id** }] [{ **src ip** | **src ip mask** | **src port** | **destination ip** | **destination ip mask** | **destination port** }] [{ **both** | **ingress** | **egress** }] [**bidirectional**]
no debug platform condition match protocol

Syntax Description

interface *interface*	Filters the output on the basis of the interface specified.
match	Enables conditional debugging for matching packets.
IPv4	(Optional) Filters the output on the basis of the specified IPv4 address.
Ipv6	(Optional) Filters the output on the basis of the specified IPv6 address.
protocol	Filters the output on the basis of the specified protocol.
tcp	(Optional) Specifies TCP to filter the output on the basis of the TCP.
udp	(Optional) Specifies UDP to filter the output on the basis of the UDP.
protocol_id	(Optional) Specifies protocol ID to filter the output on the basis of the protocol ID.
src ip	(Optional) Specifies the source IP address to filter the output on the basis of the source IP.
src ip mask	(Optional) Specifies the source IP subnet mask to filter the output on the basis of the source IP subnet mask.
destination ip	(Optional) Specifies the destination IP address to filter output on the basis of the destination IP address.
destination ip mask	(Optional) Specifies the destination IP address to filter output on the basis of the destination IP subnet mask.
destination port	(Optional) Specifies the destination port address to filter output on the basis of the destination port.
both	(Optional) Filters output on the basis of both incoming and outgoing packets.
ingress	(Optional) Filters output on the basis of incoming packets.
egress	(Optional) Filters output on the basis of outgoing packets.
bidirectional	(Optional) Filters output in both the directions.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	This command was introduced.

The following example shows how to create the equivalent bidirectional Access Control List (ACL) to match the packet flow in both directions.

```
Device# debug packet-trace condition source-ip 10.0.0.1
Device# debug packet-trace condition destination-ip 10.0.0.2
Device# debug platform condition match ipv4 host 10.0.0.1 host 10.0.0.2 both bidirectional
Device# debug packet-trace condition stop
```

debug platform condition start

To start conditional debugging on a system, use the **debug platform condition start** command in privileged EXEC mode.

debug platform condition start

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	This command was introduced.

The following example shows how to start conditional debugging on a system:

```
Device# debug platform condition interface Gi0/0/1 efp-id 100 access-list 700
Device# debug platform feature evc dataplane
Device# debug platform condition start
```

debug platform condition stop

To stop conditional debugging on a system, use the **debug platform condition stop** command in privileged EXEC mode.

debug platform condition stop

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	This command was introduced.

The following example shows how to stop conditional debugging on a system.

```
Device# debug platform condition interface Gi0/0/1 efp-id 100 access-list 700
Device# debug platform feature evc dataplane
Device# debug platform condition start
Device# debug platform condition stop
```

debug platform condition feature sdwan controlplane bfd

To start conditional debugging on a system for BFD sessions on a control plane, use the **debug platform condition feature sdwan controlplane bfd** command in privileged EXEC mode.

debug platform condition feature sdwan controlplane bfd

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.15.1a	This command was introduced.

Examples

The following example shows how to enable debugging mode for BFD sessions on a control plane:

```
Device# debug platform condition feature sdwan controlplane bfd
  ld         BFD LD
  tloc-pair  BFD tloc pair

Device# debug platform condition feature sdwan controlplane bfd ld 20008
Device# debug platform condition
Device# debug platform condition start

Device# debug platform condition feature sdwan controlplane bfd tloc-pair
encap ipsec local-color mpls remote-color mpls system-ip 172.16.255.1
debug platfom condition start
```

debug platform software sdwan fpm

To enable debugging mode for Forwarding Policy Manager, use the **debug platform software sdwan fpm** command in privileged EXEC mode. To disable debugging mode for Forwarding Policy Manager, use the **undebug** form of the command.

debug platform software sdwan fpm { **all** | **config** | **dpi** | **policy** | **ttm** }
undebug platform software sdwan fpm { **all** | **config** | **dpi** | **policy** | **ttm** }

Syntax Description

all	Controls the debugging of events related to the forwarding policy manager, including configuration changes, application-aware routing events, and communication with the tunnel table manager.
config	Controls the debugging of messages that are logged as a result of a policy configuration change made either directly on the router or because the changes have been pushed from the Cisco vSmart controller to the router.
dpi	Controls the debugging of all application-aware routing (deep packet inspection) events.
policy	Controls the debugging of messages that are logged as the result of policy programming events.
ttm	Controls the debugging of communication between the forwarding policy manager and the tunnel table manager.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Use the **debug platform software sdwan fpm** command to enable debugging mode for Forwarding Policy Manager. Debug output is placed in the *bootflash:/tracelogs* folder on the local device.

Examples

The following example shows how to enable debugging mode for Forwarding Policy Manager. After the information is collected, you can disable it, using the undebug form of the command:

```
Device# debug debug platform software sdwan fpm all
Device# undebug debug platform software sdwan fpm all
```

debug vdaemon

To enable and disable debugging mode for vdaemon software function on Cisco SD-WAN controllers. The debug output is saved to the /var/log/tmplog/vdebug file on the local device.

debug vdaemon { **all** | **cert** | **confd** | **error** | **events** | **ftm** | **hello** | **misc** | **mts** | **ncs** | **packets** | **peer** *sess-id logging module verbosity level* | **rtm** | **ssl** | **ttm** }
no debug vdaemon { **all** | **cert** | **confd** | **error** | **events** | **ftm** | **hello** | **misc** | **mts** | **ncs** | **packets** | **peer** *sess-id logging module verbosity level* | **rtm** | **ssl** | **ttm** }

Syntax Description

all	Enables the display of debugging output for all vdaemon processes.
cert	Enables the display of debugging output for vdaemon certificate functions.
confd	Enables the display of debugging output for vdaemon process CLI functions.
error	Enables the display of debugging output errors for vdaemon actions.
events	Enables the display of debugging output for vdaemon process events.
ftm	Enables the display of debugging output for vdaemon ftm actions.
hello	Enables the display of debugging output for vdaemon hello packets.
misc	Enables the display of debugging output for miscellaneous vdaemon process events.
mt	Enables the display of debugging output for vdaemon multi-tenant actions.
ncs	Enables the display of debugging output for vdaemon networked control system (NCS) actions.
packets	Enables the display of debugging output for all vdaemon process packets.
peer *sess-id logging module verbosity level*	Enables the display of debugging output for communication between peer sessions. *logging module*: verifies the logs for the peer. *verbosity level*: Enables verbose logs for the module specified only of the peer whose session id is provided.
rtm	Enables the display of debugging output for communication between the Cloud OnRamp for SaaS and the route table manager.
ssl	Enables the display of debugging output for vdaemon SSL actions.
ttm	Enables the display of debugging output for communication between the Cloud OnRamp for SaaS and the tunnel table manager.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Release 17.3.1a	This command was introduced.

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	The following new keywords are added: • ftm • mt • ncs • rtm • ssl • ttm • peer *sess-id* *logging module verbosity level*

Examples

The following is a sample output for **debug vdaemon peer** command.

```
Device# debug vdaemon peer sess-ID 22
Sess ID: 0000000012
Sess ID: 0000000022


Device# debug vdaemon ttm ?

Possible completions:
  debug     Debug logs
  error     Error logs
  notice    Notice logs
  verbose   Verbose logs
  |         Output modifiers
  <cr>

Device# debug vdaemon ttmverbose
```

debug platform software sdwan vdaemon

To enable debugging mode for vdaemon peer on Cisco SD-WAN Controllers, use the **debug platform software sdwan vdaemon peer** command in privileged EXEC mode. To disable debugging mode, use the **no** form of the command.

debug platform software sdwan vdaemon *session-id*

no debug platform software sdwan vdaemon peer *session-id*

Syntax Description

peer	Specifies the peer name.
session-id	Specifies the session ID.

Command Default None

Command Modes Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	This command was introduced.

Example

```
Device# debug platform software sdwan vdaemon peer
session-id
Device#  no debug platform software sdwan vdaemon peer
session-id
```

set platform software trace

To configure the binary trace level for one or all modules of a Cisco SD-WAN process on a specific hardware slot, issue the command **set platform software trace** in the Privileged EXEC mode.

set platform software trace *process slot module level*

Syntax Description

process	Specify a Cisco SD-WAN process. For the list of Cisco SD-WAN processes for which binary trace is supported see the table 'Supported Cisco SD-WAN Daemons' under 'Usage Guidelines'.
level	Hardware slot from which process messages must be logged.
module	Configure the trace level for one or all the modules of the process.
slot	Select one of the following trace levels: • debug: Debug messages • emergency: Emergency possible message • error: Error messages • info: Informational messages • noise: Maximum possible message • notice: Notice messages • verbose: Verbose debug messages • warning: Warning messages

Command Default Notice level

Command Modes Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command support introduced for select Cisco SD-WAN processes. See the table 'Supported Cisco SD-WAN Daemons' under 'Usage Guidelines'.
Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	New parameters are introduced for better binary configuration.

Usage Guidelines

Table 73: Supported Cisco SD-WAN Daemons

Cisco SD-WAN Daemons	Supported from Release
• fpmd • ftm • ompd • vdaemon • cfgmgr	Cisco IOS XE Catalyst SD-WAN Release 17.4.1a

Example

In the following example, the binary trace level for the 'config' module of the 'fpmd' process on the 'RP active' FRU is set to 'debug'.

```
Device# set platform software trace fpmd RP active config debug
```

set platform software trace vdaemon

To set the trace level for a specific module within a process on Cisco SD-WAN Controllers, use the **set platform software trace** command in privileged EXEC mode. The tracing functionality logs internal events. Trace files are automatically created and saved to the tracelogs subdirectory.

set platform software trace vdaemon *R0 RP verbose*

Syntax Description

R0	Specifies the route processor with slot 0.
RP	Specifies the route processor.
verbose	(Optional) Displays verbose information, meaning all information that can be displayed on the console during the process will be displayed.

Command Default Trace levels are not set.

Command Modes Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	This command was introduced.
Cisco IOS XE Release 17.12.1a	The following new modules are added: • vdaemon-cert • vdaemon-ftm • vdaemon-mt • vdaemon-ncs • vdaemon-rtm • vdaemon-ssl • vdaemon-ttm

Example

This example shows the trace level verbose for all the modules in the route processor with slot 0:

```
Device# set platform software trace vdaemon R0 vdaemon verbose
vdaemon-affinity  vdaemon-cert  vdaemon-confd  vdaemon-err
vdaemon-event     vdaemon-ftm   vdaemon-hello  vdaemon-misc
vdaemon-mt        vdaemon-ncs   vdaemon-pkt    vdaemon-pwk
vdaemon-rtm       vdaemon-ssl   vdaemon-ttm
```

This example shows the trace level verbose for all the modules in the route processor:

```
Device#  set platform software trace vdaemon RP active vdaemon verbose

vdaemon-affinity  vdaemon-cert   vdaemon-cfgdb  vdaemon-confd
vdaemon-err       vdaemon-event  vdaemon-ftm    vdaemon-hello
vdaemon-misc      vdaemon-mt     vdaemon-ncs    vdaemon-pkt
vdaemon-pwk       vdaemon-rtm    vdaemon-ssl    vdaemon-ttm
```

show sdwan control connections

To display the information about active control connections and control plane connections on Cisco IOS XE SD-WAN devices, use the **show sdwan control connections** command in privileged EXEC mode.

show sdwan control connections [**detail**]

Syntax Description

detail	(Optional) Displays detailed information about active control plane connections.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	This command was introduced.
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	Added the peer-session-id details in the control connection summary display.

Example

```
Device# show sdwan control connections detail

----------------------------------------------------------------------
LOCAL-COLOR- lte SYSTEM-IP- 172.16.255.19   PEER-PERSONALITY- vsmart
----------------------------------------------------------------------
site-id             100
domain-id           1
protocol            tl
sprivate-ip          10.0.5.19
private-port        23556
public-ip           10.0.5.19
public-port         23556
org-name            Cisco Systems Regression
state               up [Local Err: NO_ERROR] [Remote Err: NO_ERROR]
uptime              0:00:00:42
hello interval      1000
hello tolerance     12000
controller-grp-id   0
shared-region-id-set N/A
peer-session-id      0x004ff14166
```

monitor capture (access list/class map)

To configure a monitor capture specifying an access list or a class map as the core filter for the packet capture, use the **monitor capture** command in privileged EXEC mode. To disable the monitor capture with the specified access list or class map as the core filter, use the **no** form of this command.

monitor capture *capture-name* { **access-list** *access-list-name* | **class-map** *class-map-name* }
no monitor capture *capture-name* { **access-list** *access-list-name* | **class-map** *class-map-name* }

Syntax Description

capture-name	Specify the name of the capture.
access-list *access-list-name*	Specify an access list with the specified name.
class-map *class-map-name*	Specify a class map with the specified name.

Command Default

A monitor capture with the specified access list or a class map as the core filter for the packet capture is not configured.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This command was introduced.

Usage Guidelines

Configure the access list using the **ip access-list** command or the class map using the **class-map** command before using the **monitor capture** command. You can specify a class map, or an access list, or an explicit inline filter as the core filter. If you have already specified the filter when you entered the **monitor capture match** command, the command replaces the existing filter.

Examples

The following example shows how to define a core system filter using an existing access control list:

```
Device> enable
Device# configure terminal
Device(config)# ip access-list standard acl1
Device(config-std-nacl)# permit any
Device(config-std-nacl)# exit
Device(config)# exit
Device# monitor capture mycap access-list acl1
Device# end
```

The following example shows how to define a core system filter using an existing class map:

```
Device> enable
Device# configure terminal
Device(config)# ip access-list standard acl1
Device(config-std-nacl)# permit any
Device(config-std-nacl)# exit
Device(config)# class-map match-all cmap
Device(config-cmap)# match access-group name acl
Device(config-cmap)# exit
Device(config)# exit
Device# monitor capture mycap class-map classmap1
Device# end
```

Related Commands

Command	Description
class-map	Configures a class map.
ip access-list	Configures an access list.
match access-group	Configures the match criteria for a class map on the basis of the specified ACL.
monitor capture (interface/control plane)	Specifies attachment points with direction.
monitor capture match	Defines an explicit inline core filter.
permit	Sets conditions in a named IP access list.
show monitor capture	Displays packet capture details.

monitor capture (interface/control plane)

To configure monitor capture specifying an attachment point and the packet flow direction, use the **monitor capture** command in privileged EXEC mode. To disable the monitor capture with the specified attachment point and the packet flow direction, use the **no** form of this command.

monitor capture *capture-name* {**interface** *type number* | **control-plane**} {**in** | **out** | **both**}
no monitor capture *capture-name* {**interface** *type number* | **control-plane**} {**in** | **out** | **both**}

Syntax Description

capture-name	Specify the name of the capture.
interface *type number*	Specify an interface with the specified type and number as an attachment point.
control-plane	Specify a control plane as an attachment point.
in	Specifies the inbound traffic direction.
out	Specifies the outbound traffic direction.
both	Specifies both inbound and outbound traffic directions.

Command Default

The monitor packet capture filter specifying is not configured.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This command was introduced.

Usage Guidelines

Repeat the **monitor capture** command as many times as required to add multiple attachment points.

Examples

The following example shows how to add an attachment point to an interface:

```
Device> enable
Device# monitor capture mycap interface GigabitEthernet 2 in
Device# end
```

The following example shows how to add an attachment point to a control plane:

```
Device> enable
Device# monitor capture mycap control-plane out
Device# end
```

Related Commands

Command	Description
access-list	Configures an access list.
class-map	Configures a class map.
monitor capture match	Defines an explicit in-line core filter.

Command	Description
monitor capture (access list/class map)	Specifies an access list or class map as the core filter during packet capture.
show monitor capture	Displays packet capture details.

monitor capture match ipv4

To define a core filter for monitoring packet capture for IPv4 packets, use the **monitor capture match ipv4** command in privileged EXEC mode. To remove this filter, use the **no** form of this command.

monitor capture *capture-name* **match ipv4** *source-prefix/length destination-prefix/length* [**bidirectional**]

no monitor capture *capture-name* [**match**]

Syntax Description

capture-name	Name of the capture.
source-prefix/length	Network prefix and length of the IPv4 source address.
destination-prefix/length	Network prefix and length of the IPv4 destination address.
bidirectional	(Optional) Captures bidirectional packets.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command is supported for Cisco Catalyst SD-WAN.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `monitor capture match` command.

Examples

The following example shows how to define a core filter for monitoring packet capture for IPv4 packets:

```
Device# monitor capture match CISCO ipv4 198.51.100.0/24 192.0.2.0/24 bidirectional
```

monitor capture match ipv6

To define a core filter for monitoring packet capture for IPv6 packets, use the **monitor capture match ipv6** command in privileged EXEC mode. To remove this filter, use the **no** form of this command.

monitor capture *capture_name* **match ipv6** { { *ipv6-source-prefix/length* | **any** | **host** *ipv6-source-address* } { *ipv6-destination-prefix/length* | **any** | **host** *ipv6-destination-address* } | **protocol** { *protocol_num* | **tcp** | **udp** } { *ipv6-source-prefix/length* | **any** | **host** *ipv6-source-address* } [**eq** | **lt** | **gt** | **neg** | **range** *port-num*] { *ipv6-destination-prefix/length* | **any** | **host** *ipv6-destination-address* } [**eq** | **lt** | **gt** | **neg** | **range** *port-num*] } [**bidirectional**]

no monitor capture *capture_name*

Syntax Description

capture_name	Name of the capture.
interface_name	Specify GigabitEthernet IEEE 802.3z interface name.
interface_num	Specify the GigabitEthernet interface number. Range: 1 to 32.
match	Describes filters inline.
ipv6	IPv6 packets only.
ipv6-prefix/length	IPv6 source or destination prefix. Range for the Length value: 0 to 128.
host *ipv6-address*	Specifies a single source or destination IPv6 host.
protocol_num	Specifies an IP protocol number.
any	Specifies the network prefix and length of any IPv4 or IPv6 destination address.
TCP | **UDP**	Filter by TCP or UDP protocol.
eq	(Optional) Specifies that only packets with a port number that is equal to the port number associated with the IP address are matched.
lt	(Optional) Specifies that only packets with a port number that is lower than the port number associated with the IP address are matched.
gt	(Optional) Specifies that only packets with a port number that is greater than the port number associated with the IP address are matched.
neg	(Optional) Specifies that only packets with a port number that is not equal to the port number associated with the IP address are matched.
range *port-num*	(Optional) Specifies the range of port numbers. Range: 0 to 65535.
bidirectional	(Optional) Captures bidirectional packets.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This command was introduced.

Usage Guidelines

Use the **monitor capture** command to specify the core filter as a class map, access list, or explicit inline filter. Any filter has already specified before you enter the **monitor capture match** command is replaced.

Examples

The following example shows how to set a filter for IPv6 source and destination traffic:

```
Device# monitor capture test match ipv6 protocol tcp host 2001:3c0:1::71 host 2001:380:1::71
 bidirectional
```

Related Commands

Command	Description
monitor capture match ipv4	Monitor filtering and capturing of IPv4 traffic.

privilege exec level

To set the privilege level for exec commands, use the **privilege exec level** command in global configuration mode. To reset the exec command to the default privilege level of 15, use the **no** form of this command.

privilege exec level *level command*
no privilege exec level *level command*

Syntax Description

level	Privilege level 0 - 15.
command	The exec command for which you want to set thes privilege level.

Command Default

The default exec privilege level is 15.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Cisco Internetwork Operating System (IOS) currently has 16 privilege levels that range from 0 through 15. Users have access to limited commands at lower privilege levels compared to higher privilege levels. You can use this command to set the privilege level for exec commands.

Example

The following example shows how to set the exec command show logging to privilege level 1.

```
Device(config)# privilege exec level 1 show logging
```

request nms sdavc-gw

To start, stop, and perform other operations on the SD-AVC gateway service operating locally on Cisco SD-WAN Manager instances, in single-node or cluster environments, use the **request nms sdavc-gw diagnostics** command in EXEC mode.

request nms sdavc-gw diagnostics
{ **start** | **stop** | **restart** | **status** | **diagnostics** | **local_run** }

Syntax Description

start	Start the local SD-AVC gateway service.
stop	Stop the local SD-AVC gateway service.
restart	Restart the local SD-AVC gateway service.
status	Display whether the local SD-AVC gateway service is enabled, and the uptime (seconds).
diagnostics	Display diagnostics information for the SD-AVC gateway service. In a cluster environment, the output includes each node in the cluster. If you include the **local_run** keyword, the output provides information only about the local node.
local_run	When using the **diagnostics** keyword, including this causes the output to provide information only about the local node.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco Catalyst SD-WAN Manager Release 20.18.1	Added the **local_run** keyword.

Usage Guidelines

The SD-AVC gateway service operates on SD-WAN Manager instances, in single-node or cluster environments. It is distinct from the SD-AVC service.

Execute the command on the host of a SD-WAN Manager instance.

Example

This example displays diagnostic information regarding the SD-AVC gateway service. It includes the **local_run** keyword, so the output provides information only about the local node.

```
sdwan-manager# request nms sdavc-gw diagnostics local_run
NMS SDAVC gateway
------------------------------------------------------------
Running Diagnostics for vManage 1: 10.0.105.38
------------------------------------------------------------
Checking cluster connectivity for ports 8443 ...
Pinging vManage node 0 on 10.0.100.101:8443...

Starting Nping 0.7.80 ( https://nmap.org/nping ) at 2024-10-15 16:53 UTC
```

```
SENT (0.0022s) Starting TCP Handshake > 10.254.1.14:8443
RCVD (0.0025s) Handshake with 10.254.1.14:8443 completed
SENT (1.0036s) Starting TCP Handshake > 10.254.1.14:8443
RCVD (1.0040s) Handshake with 10.254.1.14:8443 completed
SENT (2.0050s) Starting TCP Handshake > 10.254.1.14:8443
RCVD (2.0053s) Handshake with 10.254.1.14:8443 completed

Max rtt: 0.384ms | Min rtt: 0.286ms | Avg rtt: 0.331ms
TCP connection attempts: 3 | Successful connections: 3 | Failed: 0 (0.00%)
Nping done: 1 IP address pinged in 2.01 seconds
Pinging vManage node 1 on 10.254.2.14:8443...

Starting Nping 0.7.80 ( https://nmap.org/nping ) at 2024-10-15 16:53 UTC
SENT (0.0019s) Starting TCP Handshake > 10.254.2.14:8443
RCVD (0.0020s) Handshake with 10.254.2.14:8443 completed
SENT (1.0031s) Starting TCP Handshake > 10.254.2.14:8443
RCVD (1.0031s) Handshake with 10.254.2.14:8443 completed
SENT (2.0044s) Starting TCP Handshake > 16910254.2.14:8443
RCVD (2.0044s) Handshake with 10.254.2.14:8443 completed

Max rtt: 0.029ms | Min rtt: 0.012ms | Avg rtt: 0.020ms
TCP connection attempts: 3 | Successful connections: 3 | Failed: 0 (0.00%)
Nping done: 1 IP address pinged in 2.00 seconds
Pinging vManage node 2 on 10.254.3.14:8443...

Starting Nping 0.7.80 ( https://nmap.org/nping ) at 2024-10-15 16:53 UTC
SENT (0.0013s) Starting TCP Handshake > 10.254.3.14:8443
RCVD (0.0018s) Handshake with 10.254.3.14:8443 completed
SENT (1.0029s) Starting TCP Handshake > 10.254.3.14:8443
RCVD (1.0033s) Handshake with 10.254.3.14:8443 completed
SENT (2.0046s) Starting TCP Handshake > 10.254.3.14:8443
RCVD (2.0052s) Handshake with 10.254.3.14:8443 completed

Max rtt: 0.555ms | Min rtt: 0.348ms | Avg rtt: 0.437ms
TCP connection attempts: 3 | Successful connections: 3 | Failed: 0 (0.00%)
Nping done: 1 IP address pinged in 2.01 seconds
Server network connections
---------------------------
tcp        0      0 10.254.2.14:8443       10.254.1.14:44022      FIN_WAIT2   19837/java

SDAVC-GW-Liveness-Check: Succeeded on port 10501
SDAVC-GW-Liveness-Check: Succeeded on port 10502
SDAVC-GW   md5sum : 4f271f7ab6
SDAVC-user md5sum : 4f271f7ab6
Passwords are In-Sync
SDAVC-GW-Status-Check: Succeeded with status CONNECTED
```

request nms patch all

To upgrade Cisco SD-WAN Manager to minor version releases use **request nms patch all** command in priviledged EXEC mode.

request nms patch all *path of patch file*

Syntax Description

patch all	Patches all NMS services
path of patch file	Specify the name of the patch image file

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco Catalyst SD-WAN Manager Release 20.15.1	This command was introduced.

Example

The following example shows how to upgrade Cisco SD-WAN Manager to minor version releases.

```
request nms patch all /home/admin/extra-packages_20.15.0-77.tar.gz
Triggering patching operation to extra-packages_20.15.0-77.tar.gz
Patch in-progress file created at /tmp/patch_in_progress
Initiating patching of pre-existing containers...
Extracting extra-packages_20.15.0-77.tar.gz...
sdavc-gw - skipped
host-agent - patched
ratelimit - skipped
statistics-db - patched
configuration-db - patched
coordination-server - patched
cloudagent-v2 - patched
support-tools - skipped
vault - skipped
messaging-server - patched
cluster-oracle - patched
data-collection-agent - patched
service-proxy - patched
upgrade-coordinator - patched
device-data-collector - patched
application-server - patched
sdavc - skipped
olap-db - patched
reporting - skipped
Patching of all containers was completed successfully.
Restarting container manager...
timeout: run: container-manager: (pid 10530) 461s, normally down, want down, got TERM
Attempt 1 to remove /var/lib/nms/docker/*
Removal of /var/lib/nms/docker/* successful
timeout: run: container-manager: (pid 1408) 7s, normally down
Verifying application server bring up was successful
Checking application-server reachability
Container 'application-server' is not running.
…
…
…
Container 'application-server' is starting.
Checking application-server reachability
Container 'application-server' is starting.
Checking application-server reachability
Container 'application-server' is starting.
Checking application-server reachability
Container 'application-server' is starting.
Checking application-server reachability
Container 'application-server' is up and healthy.
device#
```

request nms unpatch

To unpatch Cisco SD-WAN Manager from minor version releases use **request nms unpatch all** command in priviledged EXEC mode.

request nms unpatch all

Syntax Description

unpatch all	Unpatches all nms services

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco Catalyst SD-WAN Manager Release 20.15.1	This command was introduced.

Example

The following example shows how to unpatch Cisco SD-WAN Manager.

```
Device# request nms unpatch all
Initiating unpatching of containers...
Patch in-progress file created at /tmp/patch_in_progress
Extracting extra-packages.tar.gz...
Removing any old service containers...
application-server - unpatch complete
cloudagent-v2 - unpatch complete
cluster-oracle - unpatch complete
configuration-db - unpatch complete
coordination-server - unpatch complete
data-collection-agent - unpatch complete
device-data-collector - unpatch complete
host-agent - unpatch complete
messaging-server - unpatch complete
olap-db - unpatch complete
ratelimit - unpatch complete
reporting - unpatch complete
sdavc - unpatch complete
sdavc-gw - unpatch complete
service-proxy - unpatch complete
statistics-db - unpatch complete
support-tools - unpatch complete
upgrade-coordinator - unpatch complete
vault - unpatch complete
Restarting container manager...
timeout: run: container-manager: (pid 6136) 5956s, normally down, want down, got TERM
Attempt 1 to remove /var/lib/nms/docker/*
Removal of /var/lib/nms/docker/* successful
timeout: run: container-manager: (pid 10530) 7s, normally down
unpatching of all containers was completed successfully.
Verifying application server bring up was successful
Checking application-server reachability
```

```
Container 'application-server' is not running.
Checking application-server reachability
Container 'application-server' is not running.
…
…
…
 Checking application-server reachability
Container 'application-server' is not running.
Checking application-server reachability
Container 'application-server' is starting.
Checking application-server reachability
Container 'application-server' is starting.
Checking application-server reachability
Container 'application-server' is starting.
Checking application-server reachability
Container 'application-server' is starting.
Checking application-server reachability
Container 'application-server' is starting.
Checking application-server reachability
Container 'application-server' is starting.
Checking application-server reachability
Container 'application-server' is starting.
Checking application-server reachability
Container 'application-server' is starting.
Checking application-server reachability
Container 'application-server' is up and healthy.
Patch in-progress file deleted from /tmp/patch_in_progress
Device#
```

request nms container-manager diagnostics

To display diagnostic information and status for the Network Management System (NMS) containers running on Cisco SD-WAN Manager use the **request nms container-manager diagnostics** command in priviledged EXEC mode.

request nms container-manager diagnostics

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco Catalyst SD-WAN Manager Release 20.14.1	This command was introduced.

Example

The following example shows how to display diagnostic information for the NMS containers running on Cisco SD-WAN Manager.

```
Device# request nms container-manager diagnostics
NMS container manager
Checking container-manager status

Listing all images
------------------------
REPOSITORY                  TAG         IMAGE ID       CREATED        SIZE
```

```
sdwan/reporting              latest      10d3363a0c7c   15 hours ago   941MB
sdwan/messaging-server       0.20.0      30547ceba4b9   15 hours ago   150MB
sdwan/radkit                 1.8.6rc1    5ebe514b17d4   15 hours ago   782MB
sdwan/cluster-orchestrator   1.0.1       5aa1fd0e8e18   15 hours ago   669MB
sdwan/configuration-db       4.4.38      d6b9eb6fd60e   15 hours ago   548MB
sdwan/olap-db                24.3.6.48   219369311a35   15 hours ago   409MB
sdwan/cloudagent-v2          1.0.0       a56c3552ab49   15 hours ago   703MB
sdwan/upgrade-coordinator    2.0.0       d95f20da260b   15 hours ago   141MB
sdwan/application-server     24.0.1      7d505d68bf3f   15 hours ago   1.15GB
sdwan/coordination-server    3.8.4       91b45542b9e2   15 hours ago   346MB
sdwan/vault                  1.0.1       b2323a89ada8   2 weeks ago    511MB
sdavc                        4.7.0       d1512d663ac7   7 weeks ago    749MB
sdavc-gw                     4.7.0       4ed15cea64ee   7 weeks ago    463MB

Listing all containers
------------------------
CONTAINER ID   IMAGE                                 COMMAND                  CREATED
 STATUS                         PORTS

                                                                                                  NAMES
ed8024e0dbb5   sdwan/messaging-server:0.20.0         "/bin/bash /entrypoi…"   6 minutes ago
 Up 6 minutes (healthy)         127.0.0.1:4222->4222/tcp, 127.0.0.1:6222->6222/tcp,
127.0.0.1:8222->8222/tcp

messaging-server
9013b37451d9   sdwan/olap-db:24.3.6.48               "/usr/bin/tini -- /e…"   6 minutes ago
 Up 6 minutes (healthy)         127.0.0.1:8123->8123/tcp, 127.0.0.1:9363->9363/tcp

                                                                                                  olap-db
95fea11679e7   sdwan/cloudagent-v2:1.0.0             "./entrypoint.sh"        6 minutes ago
 Up 6 minutes (healthy)         127.0.0.1:9051-9052->9051-9052/tcp

                                                                                                  cloudagent-v2
2e534bbea1af   sdwan/reporting:latest                "/usr/bin/tini -g --…"   6 minutes ago
 Up 6 minutes                   80/tcp, 127.0.0.1:9080->9080/tcp

                                                                                                  reporting
b25381e8e543   sdwan/coordination-server:3.8.4       "/docker-entrypoint.…"   6 minutes ago
 Up 6 minutes (healthy)         127.0.0.1:2181->2181/tcp, 127.0.0.1:2888->2888/tcp,
127.0.0.1:3888->3888/tcp, 127.0.0.1:4888->4888/tcp

coordination-server
0b696e5f38d5   sdwan/vault:1.0.1                     "docker-entrypoint.s…"   6 minutes ago
 Up 6 minutes (healthy)         8200/tcp, 127.0.0.1:8201-8202->8201-8202/tcp

                                                                                                  vault
3c7254a24f5a   sdavc:4.7.0                           "/usr/local/bin/sdav…"   6 minutes ago
 Up About a minute (healthy)    127.0.0.1:10503->8080/tcp, 127.0.0.1:10504->8443/tcp

                                                                                                  sdavc
944e74177a8f   sdavc-gw:4.7.0                        "/bin/bash -c 'exec …"   6 minutes ago
 Up 6 minutes (healthy)         127.0.0.1:8444->8444/tcp, 127.0.0.1:10501->8080/tcp,
127.0.0.1:10502->8443/tcp, 127.0.0.1:10000->50000/udp

sdavc-gw
0c9c29dbf0a8   sdwan/configuration-db:4.4.38         "/usr/bin/tini -g --…"   6 minutes ago
 Up 6 minutes (healthy)         127.0.0.1:2004->2004/tcp, 127.0.0.1:5000->5000/tcp,
127.0.0.1:6000->6000/tcp, 127.0.0.1:6362->6362/tcp, 127.0.0.1:6372->6372/tcp,
127.0.0.1:7000->7000/tcp, 127.0.0.1:7473-7474->7473-7474/tcp,
127.0.0.1:7687-7688->7687-7688/tcp   configuration-db
c7fe7153a21a   sdwan/application-server:24.0.1       "/usr/bin/tini -g --…"   6 minutes ago
 Up 6 minutes (healthy)
```

```
base-application-server
6c8f3ec5103f   sdwan/cluster-orchestrator:1.0.1   "/entrypoint.sh"         7 minutes ago
 Up 7 minutes (healthy)        127.0.0.1:9090->9090/tcp, 127.0.0.1:9099->9099/tcp


cluster-orchestrator

Docker info
------------------------
Client:
 Context:    default
 Debug Mode: false

Server:
 Containers: 11
  Running: 11
  Paused: 0
  Stopped: 0
 Images: 13
 Server Version: 23.0.6
 Storage Driver: overlay2
  Backing Filesystem: extfs
  Supports d_type: true
  Using metacopy: false
  Native Overlay Diff: true
  userxattr: false
 Logging Driver: local
 Cgroup Driver: cgroupfs
 Cgroup Version: 1
 Plugins:
  Volume: local
  Network: bridge host ipvlan macvlan null overlay
  Log: awslogs fluentd gcplogs gelf journald json-file local logentries splunk syslog
 Swarm: inactive
 Runtimes: io.containerd.runc.v2 runc
 Default Runtime: runc
 Init Binary: docker-init
 containerd version: b1624c3628954e769dd50783b63823040b2db38c.m
 runc version: v1.1.14-0-g2c9f5602-dirty
 init version: b9f42a0-dirty
 Security Options:
  seccomp
   Profile: builtin
 Kernel Version: 6.6.21-yocto-standard
 Operating System: viptela 20.18.1 (scarthgap)
 OSType: linux
 Architecture: x86_64
 CPUs: 8
 Total Memory: 23.48GiB
 Name: vm
 ID: 7f6e3203-ad3a-40af-aacd-21e43cbe1c9c
 Docker Root Dir: /var/lib/nms/docker
 Debug Mode: false
 Registry: https://index.docker.io/v1/
 Experimental: false
 Insecure Registries:
  127.0.0.0/8
 Live Restore Enabled: false

WARNING: No cpu cfs quota support
WARNING: No cpu cfs period support
WARNING: No blkio throttle.read_bps_device support
WARNING: No blkio throttle.write_bps_device support
```

```
WARNING: No blkio throttle.read_iops_device support
WARNING: No blkio throttle.write_iops_device support
```

request platform software sdwan admin-tech

To collect system status information in a compressed tar file for troubleshooting and diagnostics, use the **request platform software sdwan admin-tech** command in privileged EXEC mode.

request platform software sdwan admin-tech
{ **exclude-certs** | **exclude-cores** | **exclude-logs** | **exclude-tech** | **timeout** }

Syntax Description

exclude-certs	Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.15.1a Do not include any certificates in the compressed tar file. Certificates are stored in the /var/crash directory on a local Cisco IOS XE Catalyst SD-WAN device.
exclude-cores	Do not include any core files in the compressed tar file. Core files are stored in the /var/crash directory on a local Cisco IOS XE Catalyst SD-WAN device.
exclude-logs	Do not include any log files in the compressed tar file. Log files are stored in the /var/log directory on a local Cisco IOS XE Catalyst SD-WAN device.
exclude-tech	Do not include any process (daemon) and operational-related files in the compressed tar file. These files are stored in the /var/tech directory on a local Cisco IOS XE Catalyst SD-WAN device.
timeout	Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.15.1a admin-tech timeout value. When the admin-tech is truncated, you can provide custom timeout value for admin-tech. Default: 30 minutes.

Command Modes

Privileged EXEC mode (#)

Command History

Release	Modification
Cisco IOS XE SD-WAN 16.10.1	Command qualified for use in Cisco SD-WAN Manager CLI templates.
Cisco IOS XE Catalyst SD-WAN Release 17.15.1a	Added the **exclude-certs** and **timeout** keywords.

Usage Guidelines

This command can be used to collect system status information in a compressed tar file for troubleshooting and diagnostics. This tar file, which is saved in the vmanage-admin's home directory, contains the output of various commands and the contents of various files on the local device, including syslog files, files for each process (daemon) running on the device, core files, and configuration rollback files. For aid in troubleshooting, send the file to Cisco SD-WAN customer support.

If your Cisco IOS XE Catalyst SD-WAN device contains a large number of crash log files, it might take a few minutes for the request admin-tech command to complete.

On a Cisco IOS XE Catalyst SD-WAN device, you can run only one request admin-tech command at a time. If a command is in progress, Cisco IOS XE Catalyst SD-WAN device does not let a second one start.

Example

The following example shows how to collect system status information in a compressed tar file for troubleshooting and diagnostics.

```
Device# request platform software sdwan admin-tech
Requested admin-tech initiated.
Created admin-tech file '/home/vmanage-admin/cEdge-20201115-110540-admin-tech.tar.gz'
IOS filename::  'bootflash:vmanage-admin/cEdge-20201115-110540-admin-tech.tar.gz'
```

Related Commands

Command	Description
admin-tech-on-failure	Collects system status information in a compressed tar file for troubleshooting and diagnostics.

request platform software sdwan auto-suspend reset

To bring all BFD sessions out of suspension, use the **request platform software sdwan auto-suspend reset** command in privileged EXEC mode.

request platform software sdwan auto-suspend reset { **local-sys-ip** *local-ip-address* **local-color** *local-color* **remote-sys-ip** *remote-ip-address* **remote-color** *remote-color* **encap** *encap-type* }

Syntax Description

local-sys-ip *local-ip-address*	Specifies the local system IP address.
local-color *local-color*	Identifier for the transport tunnel. The color specifies a specific WAN transport provider.
remote-sys-ip *remote-ip-address*	Specifies the IP address of the remote system.
remote-color *remote-color*	Specifies a WAN transport provider.
encap *encap-value*	Specifies the encapsulation type for the BFD session.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	This command was introduced.

Usage Guidelines

Use this command to bring all BFD sessions out of suspension.

Example

The following example shows how to reset a local color lte BFD session:

```
# request platform software sdwan auto-suspend reset local-color lte
```

The following example shows how to reset a BFD session with a local system IP, local color lte, and remote system IP with a remote color:

```
# request platform software sdwan auto-suspend reset local-sys-ip 172.16.12.255 local-color
 lte remote-sys-ip 10.10.1.1 remote-color 3g
```

The following example shows how to reset a BFD session with a local system IP, local color lte, remote system IP with a remote color, and an encapsulation type of IPsec:

```
# request platform software sdwan auto-suspend reset local-sys-ip 172.16.12.255 local-color
 lte remote-sys-ip 10.10.1.1 remote-color 3g encap ipsec
```

Related Commands

Command	Description
show sdwan bfd history	Displays Cisco SD-WAN BFD history.
show sdwan bfd sessions	Displays Cisco SD-WAN BFD sessions.
show sdwan bfd summary	Displays a Cisco SD-WAN BFD summary.
show sdwan bfd tloc-summary-list	Displays a Cisco SD-WAN BFD TLOC summary list.

request platform software sdwan certificate install

To install a certificate on the Cisco SD-WAN WAN Edge device, use the **request platform software sdwan certificate install** command in privileged EXEC mode.

request platform software sdwan certificate install *file-path* { **vpn** *vpn-id* }

Syntax Description

file-path	Path to the certificate file. Install the certificate in specified filename. *file-path* can be one of the following: • bootflash • flash • webui
vpn *vpn-id*	VPN in which the certificate file is located. When you include this option, one of the interfaces in the specified VPN is used to retrieve the file.

Command Default

None.

Command Modes

Privileged EXEC mode (#)

Command History

Release	Modification
Cisco IOS XE SD-WAN 16.10.1	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

This command can be used to install a certificate on a Cisco IOS XE Catalyst SD-WAN device. Certificates are used on Public Key Infrastructure (PKI) deployments.

Example

The command can be used to install a certificate on a Cisco IOS XE Catalyst SD-WAN device. Certificates are used on Public Key Infrastructure (PKI) deployments.

```
Device# request platform software sdwan certificate install bootflash:cert.csr
```

request platform software sdwan config reset

To clear the SD-WAN configuration from a Cisco IOS XE Catalyst SD-WAN device, use the **request platform software sdwan config reset** command in privileged EXEC mode.

request platform software sdwan config reset

Command Default

None

Command Modes

Privileged EXEC mode (#)

Command History

Release	Modification
Cisco IOS XE SD-WAN 16.10.1	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

This command can be used to clear the SD-WAN configuration from a Cisco IOS XE Catalyst SD-WAN device. This command is disruptive, since all the SD-WAN configurations of the Cisco IOS XE Catalyst SD-WAN device will be wiped out.

This may be needed in order to restart the PnP process.

Note In releases prior to Cisco IOS XE Catalyst SD-WAN Release 17.7.1a, the **request platform software sdwan config reset** command displayed a prompt requesting that you reload the Cisco IOS XE Catalyst SD-WAN device.

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.7.1a, you no longer see the prompt requesting you to reload the Cisco IOS XE Catalyst SD-WAN device. The Cisco IOS XE Catalyst SD-WAN device reloads automatically with an appropriate message on the console.

When this command encounters a Virtual Teletype (VTY) line without autoboot, you need to change the `config-register` value so that the autoboot bit is set as `0xXXX2`.

You can check the value of `config-register` using the **show version** or **show bootvar** commands.

```
Device# show bootvar
BOOT variable = bootflash:packages.conf,1;bootflash:prev_packages.conf,1;
CONFIG_FILE variable does not exist
BOOTLDR variable does not exist
Configuration register is 0x2102
Standby not ready to show bootvar
```

You can change the value of `config-register` by pushing the configuration to the device using a CLI add-on template or by using the CLI.

```
config-transaction
config-register 0x2102
commit
```

Example

The following example shows how to clear the SD-WAN configuration from a Cisco IOS XE Catalyst SD-WAN device.

```
Device# request platform software sdwan config reset
```

request platform software sdwan csr upload

To upload a Certificate Signing Request (CSR) to a Cisco IOS XE Catalyst SD-WAN device, use the **request platform software sdwan csr upload** command in privileged EXEC mode.

request platform software sdwan csr upload *file-path*

Syntax Description

file-path	Path of the certificate file. Upload the CSR in the file at the specified path. *file-path* can be one of the following: • bootflash • flash • webui

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE SD-WAN 16.10.1	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines This command can be used to upload a CSR to a Cisco IOS XE Catalyst SD-WAN device. They are used on Public Key Infrastructure (PKI) deployments.

Example

The following example shows how to upload a CSR to a Cisco IOS XE Catalyst SD-WAN device.

```
Device# request platform software sdwan csr upload bootflash:cert.csr
Uploading CSR via VPN 0
Generating CSR on the hardware Router ..
Enter organization-unit name            : SDWAN-Org
Re-enter organization-unit name          : SDWAN-Org
Organization-unit name differs. Certificate will be deleted. Proceed? [yes,NO] Yes
```

request platform software sdwan port_hop color

To manually request the port hopping for TLOCs with a specific color, use the **request platform software sdwan port_hop color** command in privileged EXEC mode.

request platform software sdwan port_hop color *color*

Syntax Description

color	Color of an individual WAN transport interface. Values: 3g, biz-internet, blue, bronze, custom1, custom2, custom3, default, gold, green, lte, metro-ethernet, mpls, private1, private2, private3, private4, private5, private6, public-internet, red, and silver.

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE SD-WAN 16.10.1	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines This command can be used when NAT entries become stale.

Manually rotate to the next OMP port in the group of preselected OMP port numbers when a connection cannot be established, and continue the port hopping until a connection can be established. Each connection attempt times out in about 60 seconds.

Example

The following example shows how to rotate to the next OMP port in the group of preselected OMP port numbers to the TLOC with color LTE.

```
Device# request platform software sdwan port_hop color lte
```

request platform software sdwan root-cert-chain install

To install a file containing the root certificate key chain, use the **request platform software sdwan root-cert-chain install** command in privileged EXEC mode.

request platform software sdwan root-cert-chain install *file-path* { **vpn** *vpn-id* }

Syntax Description

file-path	Install the specified file containing the root certificate chain. *file-path* can be one of the following: • bootflash • flash • webui
vpn *vpn-id*	VPN in which the certificate file is located. When you include this option, one of the interfaces in the specified VPN is used to retrieve the file.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE SD-WAN 16.10.1	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

This command can be used to install a file containing the root certificate key chain. It is used on Public Key Infrastructure (PKI) deployments.

Example

The following example shows how to install a file containing the root certificate key chain.

```
Device# request platform software sdwan root-cert-chain install bootflash:root-chain
```

Related Commands

Command	Description
request platform software sdwan root-cert-chain uninstall	Uninstalls a file containing the root certificate key chain.

request platform software sdwan root-cert-chain uninstall

To uninstall a file containing the root certificate key chain, use the **request platform software sdwan root-cert-chain uninstall** command in privileged EXEC mode.

request platform software sdwan root-cert-chain uninstall

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE SD-WAN 16.10.1	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

This command can be used to uninstall a file containing the root certificate key chain. It is used on Public Key Infrastructure (PKI) deployments.

Example

The following example shows how to uninstall a file containing the root certificate key chain.

```
Device# request platform software sdwan root-cert-chain uninstall
```

Related Commands

Command	Description
request platform software sdwan root-cert-chain install	Installs a file containing the root certificate key chain.

request platform software sdwan software activate

To activate a software image on a local Cisco IOS XE Catalyst SD-WAN device, use the **request platform software sdwan software activate** command in privileged EXEC mode.

request platform software sdwan software activate *build-number* { **clean** | **now** }

Syntax Description

build-number	Name of the software image to activate on the device.
clean	Activates the specified software image, but do not associate the existing configuration file, and do not associates any files that store information about the device history, such as log and trace files, with the newly activated software image. **Note** Beginning with Cisco IOS XE Catalyst SD-WAN Release 17.10.1a, this option is no longer supported.

now	Activates the specified software image immediately, with no prompt asking you to confirm that you want to activate. **Note** Beginning with Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, this option is no longer supported.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE SD-WAN 16.10.1	This command was introduced.
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	The **clean** option is no longer supported.
Cisco IOS XE Catalyst SD-WAN Release 17.14.1a	The **now** option is no longer supported.

Usage Guidelines

This command can be used to activate a software image on a local Cisco IOS XE Catalyst SD-WAN device through CLI. The Cisco IOS XE Catalyst SD-WAN device reloads when the activation is complete.

Example

The following example shows how to activate a software image on a local Cisco IOS XE Catalyst SD-WAN device through CLI.

```
Device# request platform software sdwan software activate 17.03.01a.0.354
```

Related Commands

Command	Description
show sdwan software	Verifies whether the software is activated.

request platform software sdwan software install

To install a software image on a Cisco IOS XE Catalyst SD-WAN device, use the **request platform software sdwan software install** command in privileged EXEC mode.

request platform software sdwan software install *file-path* { **vpn** *vpn-id* } { **reboot** { **no-sync** } } { **download-timeout** *minutes* }

Syntax Description

file-path	Installs the software image in the specified file system. The file system must be located on the local device. *file-path* can be one of the following: • bootflash • flash • webui
vpn *vpn-id*	VPN in which the image is located. When you include this option, one of the interfaces in the specified VPN is used to retrieve the software image.
reboot no-sync	Reboots the device after installation of the software image completes. By default, the device's current configuration is copied to the other hard-disk partition and is installed with the new software image. If you include the no-sync option, the software is installed in the other hard-disk partition, and it is installed with the factory-default configuration. The existing configuration and any files that store information about the device history, such as log and trace files, are not copied to the other partition. Effectively, the no-sync option restores the device to its initial factory configuration.
download-timeout *minutes*	Specifies the installation timeout value. How long to wait before cancelling requests to install software. The duration ranges from 1 through 1440 minutes (24 hours). The default time is 60 minutes.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE SD-WAN 16.10.1	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

This command can be used to install a software image on a Cisco IOS XE Catalyst SD-WAN device. Before the software is installed, the software image is verified to determine that it is valid and that it has been signed. If the verification process fails, the software image installation is not performed.

Example

The following example shows how to install a software image on a Cisco IOS XE Catalyst SD-WAN device.

```
Device# request platform software sdwan software install
bootflash:isr4300-universalk9.17.03.02.SPA.bin
```

request platform software sdwan software remove

To remove a software image from a local Cisco IOS XE Catalyst SD-WAN device, use the **request platform software sdwan software remove** command in privileged EXEC mode.

request platform software sdwan software remove *build-number*

Syntax Description

build-number	Name of the software image to delete from the device. You cannot delete the active image.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE SD-WAN 16.10.1	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

This command can be used to remove a software image from a local Cisco IOS XE Catalyst SD-WAN device. You cannot delete the active image.

Example

The following example shows how to remove a software image from a local Cisco IOS XE Catalyst SD-WAN device.

```
Device# request platform software sdwan software remove 17.03.01a.0.354
```

request platform software sdwan software secure-boot

To check and enforce the secure boot state of the system software images, use the **request platform software sdwan software secure-boot** command in privileged EXEC mode.

request platform software sdwan software secure-boot [**list** | **set** | **status**]

Syntax Description

list	Checks secure boot state and checks whether software images on the device are secure or not secure.
set	Removes insecure software images from the device and remove an insecure boot loader.
status	Displays the security status of the software images installed on the device.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	The command is deprecated.

request platform software sdwan software set-default

To set a software image as the default image on a Cisco IOS XE Catalyst SD-WAN device, use the **request platform software sdwan software set-default** command in privileged EXEC mode.

request platform software sdwan software set-default *build-number*

Syntax Description

build-number	Name of the software image to designate as the default image on a Cisco IOS XE Catalyst SD-WAN device.

Command Default

None.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE SD-WAN 16.10.1	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

This command can be used to set a software image to be the default image on a Cisco IOS XE Catalyst SD-WAN device. Performing this operation overwrites the factory-default software image, replacing it with an image of your choosing. It is recommended that you set a software image to be the default only after verifying that the software is operating as desired on a Cisco IOS XE Catalyst SD-WAN device and in your network.

Example

The following example shows how to set a software image to be the default image on a Cisco IOS XE Catalyst SD-WAN device.

```
Device# request platform software sdwan software set-default 17.03.01a.0.354
```

request platform software sdwan software upgrade-confirm

To confirm that the upgrade to a new software image is successful, use the **request platform software sdwan software upgrade-confirm** command in privileged EXEC mode.

request platform software sdwan software upgrade-confirm

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE SD-WAN 16.10.1	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

This command can be used to confirm that the upgrade to a new software image is successful. If the device configuration includes the **sdwan system upgrade-confirm** command, issuing the **request platform software sdwan software upgrade-confirm** command within the time limit configured in the **upgrade-confirm** command confirms that the upgrade to the new software image has been successful. If this command is not issued, the device reverts automatically to the previously running software image.

If you have initiated the software upgrade from Cisco SD-WAN Manager, Cisco SD-WAN Manager automatically issues the **request platform software sdwan software upgrade-confirm** command when the Cisco IOS XE Catalyst SD-WAN device finishes rebooting. If you have initiated the software upgrade

manually from the Cisco IOS XE Catalyst SD-WAN device, you issue the **request platform software sdwan software upgrade-confirm** command from the CLI.

Example

The following example shows how to confirm that the upgrade to a new software image is successful from the CLI and the device configuration includes the **sdwan system upgrade-confirm** command.

```
Device# request platform software sdwan software upgrade-confirm
```

set platform software trace

To configure the binary trace level for one or all modules of a Cisco SD-WAN process on a specific hardware slot, issue the command **set platform software trace** in the Privileged EXEC mode.

set platform software trace *process slot module trace-level*

Syntax Description	*process*

Specify a Cisco SD-WAN process.

- all: Specify all the processes
- backplaneswitch-manager: Backplane Switch Manager Process
- bt-logger: Binary-Tracing Logger Process
- btrace-manager: Btrace Manager Process
- cfgmgr: SDWAN Cfgmgr process
- chassis-manager: Chassis-Manager
- cli-agent: CLI Agent
- cxpd: SDWAN CXP process
- dbgd: SDWAN DBG process
- dbm: Database Manager
- dmiauthd: DMI Authentication Daemon
- emd: Environmental Monitoring
- flow-file-export: Flow file export
- forwarding-manager: Forwarding Manager
- fpmd: SDWAN FPM process
- ftmd: SDWAN FTM process
- host-manager: Host Manager
- htx: AppQoE HTX Process
- install-manager: Install Manager Process
- iomd: IOMD Process
- ios: IOS Process
- iox-manager: IOx Manager Process
- license-manager: License Manager Process
- logger: Logging Manager
- mdt-pubd: Model Defined Telemetry Publisher
- ncsshd_bp: NETCONF SSH Daemon BINOS Proxy Daemon
- ndbman: Netconf DataBase Manager
- nginx: Nginx Webserver Process
- ompd: SDWAN OMP process
- pluggable-services: Pluggable Services

- qfp-control-process: QFP Client Control Process
- qfp-driver: QFP Driver Process
- qfp-ha-server: QFP HA Server
- qfp-service-process: QFP Client Serivce Process
- replication-mgr: Replication Manager
- service-mgr: Service Manager Process
- shell-manager: Shell Manager
- smd: Session Manager Process
- system-integrity: system-integrity (pistisd) Process
- ttmd: SDWAN TTM process
- vdaemon: SDWAN vDaemon process
- virt-manager: Virtualization Manager

level	Hardware slot from which process messages must be logged.

module

Specify the trace level for one or all the modules of the process.

- all-modules: All trace modules
- aom: Asynchronous object manager
- backwalk: Backwalk
- bcrdu: Crimson Dynamic Update
- bcrft: Crimson Function Tracking
- bcrpgc: Crimson Profile Guided Compiling
- bidb: Interface descriptor blocks
- bipc: Inter-process communication
- bipc_tls: BIPC-TLS communication
- bso: BSO query
- btrace: Tracing
- btrace_ra: Tracing RA
- ccolib-api: CCOLIB_API
- cdllib: CLI
- chasfs: Chassis filesystem
- cond_debug: Conditional debug
- crimson-oper: Crimson operational data
- cxpd-analytics: cloudexpress analytics
- cxpd-app: cloudexpress app
- cxpd-config: cloudexpress config
- cxpd-dpi: cloudexpress dpi
- cxpd-ftm: cloudexpress ftm
- cxpd-misc: cloudexpress misc
- cxpd-omp: cloudexpress omp
- cxpd-oper: cloudexpress oper
- cxpd-rtm: cloudexpress rtm
- cxpd-telemetry: cloudexpress telemetry
- cxpd-ttm: cloudexpress ttm
- dassist: DB assist access layer
- dbal: DB access layer
- dbdm: DB dependency management

- dfs_user: DFS
- dns-resolver: DNS Resolver
- dnsclient: dnsclient library
- evlib: Event
- evutil: Event utility
- green-be: Green backend
- green-fe: Green frontend
- httpcon-curl: HTTPCON library, curl
- httpcon-main: HTTPCON library, main
- installer-api INSTALLER_API
- libmonitor: monitor library
- mqipc: Message queue
- oormon: Out of resource monitoring
- prelib: Preload
- scooby: Scooby
- serdes: Serdes
- service-dir: Service directory
- services: Services
- tdldb-assist: DB table assist library
- tdldbpersist: DB PERSISTENCE
- tdllib: Type management
- thpool: Thread Pool
- tl3_stm: TL3 software transactional memory
- ublock: Micro blocks
- uihandler: CLI command handlers
- uipeer User interface peer
- uistatus User interface peer status
- uswap: Crimson User land Swap
- vconfd: vconfd library
- vipcommon-http: common library, http
- vipcommon-misc: common library, misc
- vipcommon-mqipc: common library, mqipc

- vipcommon-msgq: common library, msgq
- vipcommon-pwk: common library, pwk
- vipcommon-rtmsg: common library, rtmsg
- vipcommon-sql: common library, sql

slot	Select one of the following trace levels: • debug: Debug messages • emergency: Emergency possible message • error: Error messages • info: Informational messages • noise: Maximum possible message • notice: Notice messages • verbose: Verbose debug messages • warning: Warning messages

Command Default

The default tracing level for all modules is **notice**.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	New keywords introduced: • cxpd-analytics: cloudexpress analytics • cxpd-app: cloudexpress app • cxpd-config: cloudexpress config • cxpd-dpi: cloudexpress dpi • cxpd-ftm: cloudexpress ftm • cxpd-misc: cloudexpress misc • cxpd-omp: cloudexpress omp • cxpd-oper: cloudexpress oper • cxpd-rtm: cloudexpress rtm • cxpd-telemetry: cloudexpress telemetry • cxpd-ttm: cloudexpress ttm
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command support introduced for select Cisco SD-WAN processes. See the table 'Supported Cisco SD-WAN Daemons' under 'Usage Guidelines'.

Usage Guidelines

Table 74: Supported Cisco SD-WAN Daemons

Cisco SD-WAN Daemons	Supported from Release
• fpmd • ftm • ompd • vdaemon • cfgmgr	Cisco IOS XE Catalyst SD-WAN Release 17.4.1a

Example

In the following example, the binary trace level for the 'config' module of the 'fpmd' process on the 'R0' FRU is set to 'debug'.

```
Device# set platform software trace fpmd R0 config debug
```

show platform software sdwan interface-alarm summary

To display a summary of interface alarms, use the **show platform software sdwan interface-alarm summary** command in privileged EXEC mode.

show platform software sdwan interface-alarm summary

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.16.1a	This command was introduced.

This sample output shows the upstream and downstream bandwidth limits and any related alarms.

```
device# show platform software sdwan interface-alarm summary
============ Interface Alarm Summary ============
Interface Name      Upstream (kbps)     Downstream (kbps)   Base Interval(s)   High
Interval(s)
GigabitEthernet1       10000              10000               300                3600
```

show aaa servers

To display the status and number of packets that are sent to and received from all public and private authentication, authorization, and accounting (AAA) RADIUS servers as interpreted by the AAA Server MIB, use the **show aaa servers** command in user EXEC or privileged EXEC mode.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	This command was introduced.

Usage Guidelines

For more information about this command, see the Cisco IOS XE show aaa servers

Examples

The following is sample output from the **show aaa servers private** command. Only the first four lines of the display pertain to the status of private RADIUS servers, and the output fields in this part of the display are described in the table below.

```
Device# show aaa server private
RADIUS: id 24, priority 1, host 172.31.164.120, auth-port 1645, acct-port 1646
     State: current UP, duration 375742s, previous duration 0s
     Dead: total time 0s, count 0
     Quarantined: No
     Authen: request 5, timeouts 1, failover 0, retransmission 1
             Response: accept 4, reject 0, challenge 0
             Response: unexpected 0, server error 0, incorrect 0, time 14ms
             Transaction: success 4, 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 5, timeouts 0, failover 0, retransmission 0
             Request: start 3, interim 0, stop 2
             Response: start 3, interim 0, stop 2
             Response: unexpected 0, server error 0, incorrect 0, time 12ms
             Transaction: success 5, failure 0
             Throttled: transaction 0, timeout 0, failure 0
     Elapsed time since counters last cleared: 4d8h22m
     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
     Requests per minute past 24 hours:
             high - 8 hours, 22 minutes ago: 0
             low  - 8 hours, 22 minutes ago: 0
             average: 0
```

show autoip status

To display the status of automatic IP address detection for a device and display information that is detected, use the **show autoip status** command in privileged EXEC mode.

show autoip status

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Examples The following is sample output from the **show autoip status** command when an available IP address has been detected:

```
Device# show autoip status

============================
AutoIP process is stopped
============================
Last status       :success
Finally in use    :
IP address        : 192.168.0.6
Gateway IP address: 192.168.0.3
Subnet            : 192.168.47.0
Subnet mask       : 255.255.255.0
DNS server1       : 8.8.8.8
DNS server 2      : 8.8.4.4
Interface         : GigabitEthernet0/0/0
```

The following is sample output from the **show autoip status** command when detection is in progress:

```
Device# show autoip status

============================
AutoIP process is running
============================
Last status       :fail
Currently in use  :
IP address        : 192.168.1.2
Gateway IP address: 192.168.1.1
Subnet            : 192.168.40.0
Subnet mask       : 255.255.255.0
DNS server1       : 8.8.8.8
DNS server 2      : 8.8.4.4
Interface         : GigabitEthernet0/0/0
```

show class map type inspect

To display Layer 3 and Layer 4 or Layer 7 (application-specific) inspect type class maps and their matching criteria, use the **show class map type inspect** command in privileged EXEC mode.

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	This command is supported in Cisco Catalyst SD-WAN

Usage Guidelines

For usage guidelines, see the Cisco IOS XE show class-map type inspect command.

Example

The following example displays the Layer 3 and Layer 4 or Layer 7 (application-specific) inspect type class maps and their matching criteria.

```
Device# show class-map type inspect
 Class Map type inspect match-all seq_1-seq-11-cm_ (id 2)
   Match access-group name seq_1-seq-Rule_3-acl_

 Class Map type inspect match-all seq_1-seq-1-cm_ (id 1)
   Match access-group name seq_1-seq-rule1-v6-acl_
```

show cellular

To display information about the Global Navigation Satellite System (GNSS) configuration, use the **show cellular** command in privileged EXEC (#) mode.

show cellular *slot_number*

Syntax Description

gps detail	Shows the GNSS details.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.15.1a	This command is supported in Cisco Catalyst SD-WAN.

Examples

The following sample output displays the GNSS details such as feature status, mode, constellation configuration, GPS port selection, current GPS status, location coordinates, timestamp, and details of individual satellites such as GPS, GLONASS, Galileo, and BeiDou.

```
Device# show cellular 0/3/0 gps detail
GPS Feature = enabled
GPS Mode Configured = standalone
Current Constellation Configured = gnss
GPS Port Selected = Dedicated GPS port
GPS Status = GPS coordinates acquired
Last Location Fix Error = Offline [0x0]
Latitude = 37 Deg 25 Min 6.0448 Sec North
Longitude = 121 Deg 55 Min 9.6295 Sec West
Timestamp (GMT) = Fri Jul 12 16:11:30 2024
```

```
Fix type = 2D, Height = 20m
HDOP = 0.7, GPS Mode Used = standalone

Satellite Info
----------------
GPS:
Satellite #5, elevation 60, azimuth 108, SNR 31 *
Satellite #11, elevation 24, azimuth 50, SNR 34 *
Satellite #12, elevation 40, azimuth 163, SNR 33 *
Satellite #15, elevation 1, azimuth 151, SNR 19 *
Satellite #18, elevation 30, azimuth 248, SNR 33 *
Satellite #20, elevation 46, azimuth 59, SNR 36 *
Satellite #25, elevation 64, azimuth 206, SNR 35 *
Satellite #26, elevation 6, azimuth 320, SNR 27 *
Satellite #28, elevation 13, azimuth 274, SNR 33 *
Satellite #29, elevation 59, azimuth 327, SNR 37 *
Satellite #31, elevation 8, azimuth 305, SNR 27 *
Satellite #46, elevation 0, azimuth 0, SNR 34 **
Glonass:
Satellite #74, elevation 35, azimuth 312, SNR 34 *
Satellite #82, elevation 21, azimuth 52, SNR 35 *
Satellite #73, elevation 52, azimuth 248, SNR 41 *
Satellite #80, elevation 20, azimuth 187, SNR 34 *
Satellite #84, elevation 30, azimuth 278, SNR 22
Satellite #83, elevation 51, azimuth 9, SNR 27 *
Satellite #67, elevation 24, azimuth 61, SNR 36 *
Satellite #66, elevation 2, azimuth 16, SNR 0
Satellite #68, elevation 21, azimuth 115, SNR 0
Galileo:
Satellite #13, elevation 33, azimuth 247, SNR 38 *
Satellite #15, elevation 75, azimuth 330, SNR 39 *
Satellite #27, elevation 68, azimuth 271, SNR 37 *
Satellite #3, elevation 2, azimuth 118, SNR 0
Satellite #5, elevation 4, azimuth 71, SNR 0 *
Satellite #21, elevation 21, azimuth 316, SNR 0
Satellite #30, elevation 42, azimuth 164, SNR 0
Beidou:
Satellite #6, elevation 3, azimuth 322, SNR 30
Satellite #12, elevation 15, azimuth 274, SNR 30 *
Satellite #19, elevation 33, azimuth 108, SNR 0
Satellite #20, elevation 21, azimuth 54, SNR 0 *
Satellite #22, elevation 14, azimuth 161, SNR 0
Satellite #24, elevation 28, azimuth 295, SNR 0
Satellite #26, elevation 37, azimuth 232, SNR 0 *
Satellite #29, elevation 25, azimuth 73, SNR 0 *
```

show clock

To display view the system clock on a device, use the **show clock** command in privileged EXEC mode.

show clock

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This command was introduced.

Examples

The following sample output displays the system clock with the date and time.

```
Device# show clock
*00:42:53.470 UTC Tue Jul 26 2022
```

show config-pull history

To display information about success or failure of the validation and application of a configuration on Cisco Catalyst SD-WAN Controller, use the command **show config-pull history** in the privileged EXEC mode.

Command Syntax

show config-pull history [**detail**]

Syntax Description

detail	Displays detailed output information.

Output Fields

The output fields are self-explanatory.

Command Default

NA

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.18.1a	This command is introduced.

Examples

In the following sample output, the **START TIME** column indicates the duration for validation and apply stages. The **RESULT**column, indicates the success or failure at the validation and apply stages.

```
vsmart#show config-pull history details
 ID  START TIME           TENANT   STAGE     DURATION  RESULT
-------------------------------------------------------------
1   2025-01-26T03:49:15  default  validate  21        success
2   2025-01-26T03:49:37  default  apply     41        success
```

```
3   2025-01-26T04:14:25  default  validate  5         success
4   2025-01-26T04:16:28  default  apply     5         success
5   2025-01-26T04:43:01  default  rollback  5         success
6   2025-01-26T05:20:54  default  validate  5         success
7   2025-01-26T05:21:28  default  apply     5         failure
8   2025-01-26T05:25:16  default  validate  222       success
9   2025-01-26T05:29:01  default  apply     311       success
10  2025-01-26T05:58:04  default  rollback  89        success
                                                      AFFINITY
```

Show config-pull transactions

To display information about each transaction and progress of intermittent stages during validation and application of a configuration on Cisco Catalyst SD-WAN Controllers, use the command **show config-pull transaction** in the privileged EXEC mode.

Command Syntax

show config-pull transaction [**activity** | **details**]

Syntax Description

acivity	Lists the routing information about all OMP peering sessions on the local device.
detail	Displays detailed output information.

Note The results of **config-pull transaction** may not be persistent across Cisco SD-WAN Controllers after reboot.

Output Fields

The output fields are self-explanatory.

Command Default NA

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.18.1a	This command is introduced.

Examples

In the following sample output, the **TYPE** column indicates the intermittent stages of validation, application and rollback. The **MESSAGE** column, indicates the details of duration for validation and apply, and rollback stages.

```
vsmart#show config-pull transactions activity
 ID  TIMESTAMP                TYPE                  MESSAGE
--------------------------------------------------------------------------------
1   2025-01-26T03:49:20.124  validate-in-progress  Time elapsed: 5 secs
    2025-01-26T03:49:24.302  validate-in-progress  Time elapsed: 9 secs
    2025-01-26T03:49:32.461  validate-in-progress  Time elapsed: 17 secs
    2025-01-26T03:49:36.626  validate-success      Config validation success
    2025-01-26T03:49:41.752  apply-in-progress     Time elapsed: 4 secs
    2025-01-26T03:49:45.917  apply-in-progress     Time elapsed: 8 secs
    2025-01-26T03:49:54.094  apply-in-progress     Time elapsed: 17 secs
    2025-01-26T03:50:10.332  apply-in-progress     Time elapsed: 33 secs
    2025-01-26T03:50:18.521  apply-success         OMP readiness check progress 100%
2   2025-01-26T04:14:29.874  validate-success      Config validation success
    2025-01-26T04:16:32.677  apply-in-progress     Config commit success
    2025-01-26T04:16:32.829  apply-success         OMP readiness check progress 100%
    2025-01-26T04:43:06.302  rollback-success      Config rollback success
3   2025-01-26T05:20:59.286  validate-success      Config validation success
    2025-01-26T05:21:32.906  apply-in-progress     Config commit success
    2025-01-26T05:21:33.053  apply-success         OMP readiness check progress 100%
4   2025-01-26T05:25:21.706  validate-in-progress  Time elapsed: 4 secs
    2025-01-26T05:25:28.439  validate-in-progress  Time elapsed: 11 secs
    2025-01-26T05:25:38.833  validate-in-progress  Time elapsed: 21 secs
    2025-01-26T05:25:57.185  validate-in-progress  Time elapsed: 40 secs
    2025-01-26T05:26:31.392  validate-in-progress  Time elapsed: 74 secs
    2025-01-26T05:26:37.669  validate-in-progress  Time elapsed: 80 secs
    2025-01-26T05:26:47.908  validate-in-progress  Time elapsed: 90 secs
    2025-01-26T05:27:06.332  validate-in-progress  Time elapsed: 109 secs
    2025-01-26T05:27:40.519  validate-in-progress  Time elapsed: 143 secs
    2025-01-26T05:27:46.832  validate-in-progress  Time elapsed: 149 secs
    2025-01-26T05:27:57.390  validate-in-progress  Time elapsed: 160 secs
    2025-01-26T05:28:15.679  validate-in-progress  Time elapsed: 178 secs
    2025-01-26T05:28:49.962  validate-in-progress  Time elapsed: 212 secs
    2025-01-26T05:28:56.554  validate-success      Config validation success
    2025-01-26T05:29:06.243  apply-in-progress     Time elapsed: 4 secs
    2025-01-26T05:29:12.596  apply-in-progress     Time elapsed: 10 secs
    2025-01-26T05:29:22.752  apply-in-progress     Time elapsed: 20 secs
    2025-01-26T05:29:41.168  apply-in-progress     Time elapsed: 39 secs
    2025-01-26T05:30:15.455  apply-in-progress     Time elapsed: 73 secs
    2025-01-26T05:30:21.705  apply-in-progress     Time elapsed: 79 secs
    2025-01-26T05:30:32.153  apply-in-progress     Time elapsed: 90 secs
    2025-01-26T05:30:50.448  apply-in-progress     Time elapsed: 108 secs
    2025-01-26T05:31:24.537  apply-in-progress     Time elapsed: 142 secs
    2025-01-26T05:31:30.628  apply-in-progress     Time elapsed: 148 secs
    2025-01-26T05:31:40.870  apply-in-progress     Time elapsed: 158 secs
    2025-01-26T05:31:58.906  apply-in-progress     Time elapsed: 176 secs
    2025-01-26T05:32:33.311  apply-in-progress     Time elapsed: 211 secs
    2025-01-26T05:32:39.671  apply-in-progress     Time elapsed: 217 secs
    2025-01-26T05:32:50.104  apply-in-progress     Time elapsed: 228 secs
    2025-01-26T05:33:08.208  apply-in-progress     Time elapsed: 246 secs
    2025-01-26T05:33:42.515  apply-in-progress     Time elapsed: 280 secs
    2025-01-26T05:33:48.768  apply-in-progress     Time elapsed: 286 secs
    2025-01-26T05:33:59.890  apply-in-progress     Time elapsed: 297 secs
    2025-01-26T05:34:10.101  apply-success         OMP readiness check progress 100%
    2025-01-26T05:58:09.411  rollback-in-progress  Time elapsed: 4 secs
    2025-01-26T05:58:15.680  rollback-in-progress  Time elapsed: 10 secs
    2025-01-26T05:58:25.863  rollback-in-progress  Time elapsed: 20 secs
```

```
    2025-01-26T05:58:44.502  rollback-in-progress  Time elapsed: 39 secs
    2025-01-26T05:59:18.653  rollback-in-progress  Time elapsed: 73 secs
    2025-01-26T05:59:24.817  rollback-in-progress  Time elapsed: 79 secs
    2025-01-26T05:59:30.945  rollback-success      Config rollback success
                                                              AFFINITY
```

In the following sample output for a single tenant, **TXN ID** is a unique transaction ID and the type of transaction through various intermittent stages. The **TENANT** row provides the name of the tenant.

```
vsmart# show config-pull transactions detail
config-pull transactions 1
 txn-id
vsmart-config%db680ce3-6d0e-4bff-8ec4-094b182ab523%357be208-e4d7-41e4-8cfb-b985ff46a497
 tenant     default
 start-time 2025-01-26T03:49:15
 activity 2025-01-26T03:49:20.124
  type    validate-in-progress
  message "Time elapsed: 5 secs"
 activity 2025-01-26T03:49:24.302
  type    validate-in-progress
  message "Time elapsed: 9 secs"
 activity 2025-01-26T03:49:32.461
  type    validate-in-progress
  message "Time elapsed: 17 secs"
 activity 2025-01-26T03:49:36.626
  type    validate-success
  message "Config validation success"
 activity 2025-01-26T03:49:41.752
  type    apply-in-progress
  message "Time elapsed: 4 secs"
 activity 2025-01-26T03:49:45.917
  type    apply-in-progress
  message "Time elapsed: 8 secs"
 activity 2025-01-26T03:49:54.094
  type    apply-in-progress
  message "Time elapsed: 17 secs"
 activity 2025-01-26T03:50:10.332
  type    apply-in-progress
  message "Time elapsed: 33 secs"
 activity 2025-01-26T03:50:18.521
  type    apply-success
  message "OMP readiness check progress 100%"
```

In the following sample output for multitenant, the **TXN ID** is unique and tracks the progress through various intermittent states. The **TENANT** column, provides the name of the tenant.

```
vsmart# show config-pull transactions detail
 config-pull transactions 1

 txn-id
vsmart-config%push_feature_template_configuration-2eaf0422-0a58-4ed3-8330-e8deacdc93df%bceb
c683-d7da-4a16-873c-190f21261727%eea0bbbe-58d0-442f-a112-02f621ba24e3

 txn-label  4008009798

 tenant     default
```

```
 start-time 2025-03-20T01:59:12

 activity 2025-03-20T01:59:18.113

  type    validate-success

  message "Config validation success"

 activity 2025-03-20T01:59:24.084

  type    apply-in-progress

  message "Config commit success"

 activity 2025-03-20T01:59:24.875

  type    apply-success

  message "OMP readiness check progress 100%"

config-pull transactions 2

 txn-id
vsmart-config%push_feature_template_configuration-6606a25a-983d-4823-9813-eb2436cdd655%bceb
c683-d7da-4a16-873c-190f21261727%eea0bbbe-58d0-442f-a112-02f621ba24e3

 txn-label  135951754

 tenant     default

 start-time 2025-03-20T02:04:17

 activity 2025-03-20T02:04:22.764

  type    validate-success

  message "Config validation success"

 activity 2025-03-20T02:04:28.933

  type    apply-in-progress

  message "Config commit success"

 activity 2025-03-20T02:04:41.684
  type    apply-success

  message "OMP readiness check progress 100%"

config-pull transactions 3

 txn-id
vsmart-tenant-config%vsmart_policy_config-f58b9e13-a530-42d2-bd55-af6e0fd72248%bcebc683-d7d
a-4a16-873c-190f21261727%eea0bbbe-58d0-442f-a112-02f621ba24e3%centralized-policy%08bf2749-2e3c-402d-bf1
2-17f597db4ded%policy-activate%%false

 txn-label  958054532

 tenant     "vIPtela Inc Regression-Tenant1 Inc"

 start-time 2025-03-20T05:38:39

 activity 2025-03-20T05:38:44.675
```

```
  type    validate-success

  message "Config validation success"

 activity 2025-03-20T05:38:50.604

  type    apply-in-progress

  message "Config commit success"

 activity 2025-03-20T05:38:51.238

  type    apply-success

  message "OMP readiness check progress 100%"

config-pull transactions 4

 txn-id
vsmart-tenant-config%vsmart_policy_config-7384e045-d1bc-464f-a960-e6423e96e5c0%bcebc683-d7d
a-4a16-873c-190f21261727%eea0bbbe-58d0-442f-a112-02f621ba24e3%centralized-policy%3e6d3111-63fd-43c4-abf
7-2311f8b33c4a%policy-activate%%false

 txn-label  2077299990

 tenant     "vIPtela Inc Regression-Tenant3 Inc"

 start-time 2025-03-20T05:39:36

 activity 2025-03-20T05:39:41.246

  type    validate-success
  message "Config validation success"

 activity 2025-03-20T05:39:47.174

  type    apply-in-progress

  message "Config commit success"

 activity 2025-03-20T05:39:47.800

  type    apply-success

  message "OMP readiness check progress 100%"

config-pull transactions 5

 txn-id
vsmart-tenant-config%vsmart_policy_config-3a7e44b4-55a9-4116-a867-e2a5517ab2e7%bcebc683-d7d
a-4a16-873c-190f21261727%eea0bbbe-58d0-442f-a112-02f621ba24e3%centralized-policy%69a1ea59-038f-4e92-9e7
e-f51bd0e5cf18%policy-activate%%false

 txn-label  1922803485

 tenant     "vIPtela Inc Regression-Tenant5 Inc"

 start-time 2025-03-20T05:43:10

 activity 2025-03-20T05:43:16.077

  type    validate-success

  message "Config validation success"
```

```
 activity 2025-03-20T05:43:21.931
  type    apply-in-progress
  message "Config commit success"
 activity 2025-03-20T05:43:22.562
  type    apply-success
  message "OMP readiness check progress 100%"
```

show configuration commit list

To display the configuration commit list, use the **show configuration commit list** command in global configuration mode.

show configuration commit list

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This command was introduced.

Examples

The following sample output displays the configuration commit list.

```
Device(config)# show configuration commit list
2022-07-26 00:41:21

SNo. ID       User       Client      Time Stamp          Label       Comment

~~~~ ~~       ~~~~       ~~~~~~      ~~~~~~~~~~          ~~~~~       ~~~~~~~

0    10001    vmanage-ad netconf     2022-05-12 10:17:03

1    10014    vmanage-ad netconf     2022-04-04 06:36:45

2    10013    vmanage-ad netconf     2022-04-04 06:20:41

3    10012    vmanage-ad netconf     2022-04-04 06:20:38

4    10011    admin      cli         2022-03-27 21:02:40

5    10010    admin      cli         2022-03-27 20:14:42

6    10009    admin      cli         2022-03-27 20:12:57

7    10008    admin      cli         2022-03-27 20:11:21
```

```
8    10007    cfgmgr     system      2022-03-27 20:10:21

9    10006    system     system      2022-03-27 19:57:34

10   10005    system     system      2022-03-27 19:57:32

11   10004    system     system      2022-03-27 19:57:31

12   10003    system     system      2022-03-27 19:57:30

13   10002    system     system      2022-03-27 19:57:30

14   10001    system     system      2022-03-27 19:57:28

15   10000    dmidlib_sy system      2022-03-27 19:57:25
```

show crypto ipsec sa

To display the settings used by IPsec security associations (SAs), use the **show crypto ipsec sa** command in privileged EXEC mode.

Supported Parameters

active	(Optional) Displays high availability (HA)-enabled IPsec SAs that are in the active state.
address	(Optional) Displays all existing SAs. The SAs are sorted by the destination address (either the local address or the address of the IPsec remote peer) and then by protocol (Authentication Header [AH] or Encapsulation Security Protocol [ESP]).
detail	(Optional) Displays detailed information of all settings.
identity [**detail**]	(Optional) Displays only the flow information. The SA information isn't displayed.
interface *type number*	(Optional) Displays all SAs created for an interface type. The interface types are: **ATM**, **Dialer**, **GigabitEthernet**, **Loopback**, **Serial**, **Vlan**, **VirtualPortGroup**.
ipv6	(Optional) Displays IPv6 IPsec SA information.
detailed	(Optional) Displays detailed error counters.
platform	(Optional) Displays platform-specific information about the IPsec flow.
ipv4-address	(Optional) Displays IPsec SAs for an IPv4 peer.
ipv6-address	(Optional) Displays IPsec SAs for an IPv6 peer.
map *map-name* [**detail**]	(Optional) Displays any existing SAs that were created for the crypto map set using a value for the *map-name* argument.

peer [**detail** | [**vrf** *vrf*] [*ipv4-address* [**detail**] | *ipv6-address* [**detail** | **platform**]]]	(Optional) Displays all existing SAs with the peer IP address.
standby	(Optional) Displays HA-enabled IPsec SAs that are in the standby state.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco vManage CLI templates and modified the display of current outbound SPI and SPI entries.

Usage Guidelines

For more information about this command, see the Cisco IOS XE show crypto ipsec sa command.

Examples

Example 1:

The following sample output from the **show crypto ipsec sa** command shows that the SPI values isn't valid or displayed for Cisco SD-WAN IPSec tunnels.

```
Device# show crypto ipsec sa
interface: Tunnel1
    Crypto map tag: Tunnel1-vesen-head-0, local addr 10.1.15.15

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.1.15.15/255.255.255.255/0/12346)
   remote ident (addr/mask/prot/port): (10.1.16.16/255.255.255.255/0/12366)
   current_peer 10.1.16.16 port 12366
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 449884, #pkts encrypt: 449884, #pkts digest: 449884
    #pkts decaps: 449874, #pkts decrypt: 449874, #pkts verify: 449874
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 10.1.15.15, remote crypto endpt.: 10.1.16.16
     plaintext mtu 1438, path mtu 1480, ip mtu 1480, ip mtu idb Tunnel1
     current outbound spi:  [Not Available]
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: [Not Available]
        transform: esp-gcm 256 ,
        in use settings ={Transport UDP-Encaps, esn}
        conn id: 2003, flow_id: CSR:3, sibling_flags FFFFFFFF80000008, crypto map:
Tunnel1-vesen-head-0
        sa timing: remaining key lifetime is not applicable
        Kilobyte Volume Rekey has been disabled
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

      inbound ah sas:

      inbound pcp sas:

      outbound esp sas:
       spi: [Not Available]
        transform: esp-gcm 256 ,
        in use settings ={{Transport UDP-Encaps, esn}
```

```
        conn id: 2003, flow_id: CSR:3, sibling_flags FFFFFFFF80000008, crypto map:
Tunnel1-vesen-head-0
        sa timing: remaining key lifetime is not applicable
        Kilobyte Volume Rekey has been disabled
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

      outbound ah sas:

      outbound pcp sas:
```

Example 2:

The following is a sample output from the **show crypto ipsec sa** command that shows an IKE-based IPSec tunnel.

```
Device# show crypto ipsec sa
interface: Tunnel100
    Crypto map tag: Tunnel100-head-0, local addr 192.168.70.11

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.70.11/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (192.168.70.12/255.255.255.255/47/0)
   current_peer 192.168.70.12 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 2292, #pkts encrypt: 2292, #pkts digest: 2292
    #pkts decaps: 112, #pkts decrypt: 112, #pkts verify: 112
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 192.168.70.11, remote crypto endpt.: 192.168.70.12
     plaintext mtu 1446, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet2
     current outbound spi: 0x19967EA7(429293223)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0xB13A9E4F(2973408847)
       transform: esp-gcm 256 ,
        in use settings ={Tunnel, }
        conn id: 2003, flow_id: CSR:3, sibling_flags FFFFFFFF80000048, crypto map:
Tunnel100-head-0
        sa timing: remaining key lifetime 24 days, 23 hours, 41 mins
        Kilobyte Volume Rekey has been disabled
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x19967EA7(429293223)
        transform: esp-gcm 256 ,
        in use settings ={Tunnel, }
        conn id: 2004, flow_id: CSR:4, sibling_flags FFFFFFFF80000048, crypto map:
Tunnel100-head-0
        sa timing: remaining key lifetime 24 days, 23 hours, 41 mins
        Kilobyte Volume Rekey has been disabled
        IV size: 8 bytes
        replay detection support: Y
```

```
        Status: ACTIVE(ACTIVE)

    outbound ah sas:

    outbound pcp sas:
```

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

Table 75: show crypto ipsec sa Field Descriptions

Field	Description
interface	Interface on which the SA is created.
Crypto map tag	Policy tag for IPsec.
protected vrf	IVRF name that applies to the IPsec interface.
local ident (addr/mask/prot/port)	Local selector that is used for encryption and decryption.
remote ident (addr/mask/prot/port)	Remote selector that is used for encryption and decryption.
Group	Name of the GDOI group corresponding to the IPsec SA.
current_peer	Peer that communicates with the IPsec tunnel.
PERMIT, flags	Indicates that the IPsec SA is triggered by the access control list (ACL) permit action.
pkts encaps	Number of packets that were successfully encapsulated by IPsec.
pkts encrypt	Number of packets that were successfully encrypted by IPsec.
pkts digest	Number of packets that were successfully hash digested by IPsec.
pkts decaps	Number of packets that were successfully decapsulated by IPsec.
pkts decrypt	Number of packets that were successfully decrypted by IPsec.
pkts verify	Number of received packets that passed the hash digest check.
pkts compressed	Number of packets that were successfully compressed by IPsec.
pkts decompressed	Number of packets that were successfully decompressed by IPsec.
pkts not compressed	Number of outbound packets that weren’t compressed.
pkts compr. failed	Number of packets that failed compression by IPsec.
pkts not decompressed	Number of inbound packets that weren’t compressed.
pkts decompress failed	Number of packets that failed decompression by IPSec.
send errors	Number of outbound packets with errors.
recv errors	Number of inbound packets with errors.

Field	Description
local crypto endpt.	Local endpoint terminated by IPsec.
remote crypto endpt.	Remote endpoint terminated by IPsec.
path mtu	MTU size that is calculated based on the Internet Control Message Protocol (ICMP) unreachable packet, including the IPsec overhead, if any.
ip mtu	Interface MTU size that depends on the IPsec overhead.
ip mtu idb	Interface description block (IDB) that is used to determine the crypto IP MTU.
current outbound spi	Current outbound Security Parameters Index (SPI). This value isn't valid and is set to "Not Available".
inbound esp sas	Encapsulating Security Payload (ESP) for the SA for the inbound traffic.
spi	SPI for classifying the inbound packet. This value isn't valid and is set to "Not Available".
transform	Security algorithm that is used to provide authentication, integrity, and confidentiality.
in use settings	Transform that the SA uses (such as tunnel mode, transport mode, UDP-encapsulated tunnel mode, or UDP-encapsulated transport mode).
conn id	ID that is stored in the crypto engine to identify the IPsec/Internet Key Exchange (IKE) SA.
flow_id	SA identity.
crypto map	Policy for IPsec.
sa timing: remaining key lifetime (k/sec)	Seconds or kilobytes remaining before a rekey occurs.
HA last key lifetime sent (k)	Last stored kilobytes lifetime value for HA.
ike_cookies	ID that identifies the IKE SAs.
IV size	Size of the initialization vector (IV) that is used for the cryptographic synchronization data used to encrypt the payload.
replay detection support	Replay detection feature enabled by a specific SA.
Status	Indicates whether the SA is active.
inbound ah sas	Authentication algorithm for the SA for inbound traffic.

Field	Description
inbound pcp sas	Compression algorithm for the SA for inbound traffic.
outbound esp sas	Encapsulating security payload for the SA for outbound traffic.
outbound ah sas	Authentication algorithm for the SA for outbound traffic.
outbound pcp sas	Compression algorithm for the SA for outbound traffic.
DENY, flags	Indicates that the IPsec SA is triggered by the ACL deny action.
pkts decompress failed	Packets decompressed by IPsec that failed.
pkts no sa (send)	Outbound packets that couldn't find the associated IPsec SA.
pkts invalid sa (rcv)	Received packets that failed the IPsec format check.
pkts invalid prot (recv)	Received packets that have the wrong protocol field.
pkts verify failed	Received packets that failed the hash digest check.
pkts invalid identity (recv)	Packets that couldn't find the associated selector after decryption.
pkts invalid len (rcv)	Inbound packets that have an incorrect pad length for the software crypto engine.
pkts replay rollover (send)	Sent packets that failed the replay test check.
pkts replay rollover (rcv)	Received packets that failed the replay test check.
pkts internal err (send)	Sent packets that failed because of a software or hardware error.
pkts internal err (rcv)	Received packets that failed because of a software or hardware error.
protected vrf	IVRF name that applies to the IPsec interface.
pkts tagged (send)	Packets tagged with a Cisco TrustSec SGT in the outbound direction.
pkts untagged (rcv)	Packets not tagged with a Cisco TrustSec SGT in the inbound direction.

show cts environment-data

To display the TrustSec environment data, use the **show cts environment-data** command in user EXEC or privileged EXEC mode

show cts environment-data

Command Default None

Command Modes User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	This command was introduced.

Examples

The following sample outputs displays the environment data.

```
Device# show cts environment-data

 CTS Environment Data

====================

Current state = START

Last status = In Progress

Environment data is empty

State Machine is running

Retry_timer (60 secs) is not running
```

show cts pac

To display the Protected Access Credentials (PACs), use the **show cts pacs** command in user EXEC or privileged EXEC mode

Command Default

None

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	This command was introduced.

Usage Guidelines

Use this command to identify the Network Device Admission Control (NDAC) authenticator and to verify NDAC completion.

Examples

The following sample output displays the Protected Access Credential (PAC) received from a Cisco ACS with the authenticator ID (A-ID–Info):

```
Device# show cts pac

 AID: 1100E046659D4275B644BF946EFA49CD
```

```
PAC-Info:
PAC-type = Cisco Trustsec
AID: 1100E046659D4275B644BF946EFA49CD
I-ID: device1
A-ID-Info: acs1
Credential Lifetime: 13:59:27 PDT Jun 5 2010
PAC-Opaque: 000200B000030001000400101100E046659D4275B644BF946EFA49CD0006009400
0301008285A14CB259CA096487096D68D5F34D000000014C09A6AA00093A808ACA80B39EB656AF0B
CA91F3564DF540447A11F9ECDFA4AEC3A193769B80066832495B8C40F6B5B46B685A68411B7DF049
A32F2B03F89ECF948AC4BB85CF855CA186BEF8E2A8C69A7C0BE1BDF6EC27D826896A31821A7BA523
C8BD90072CB8A8D0334F004D4B627D33001B0519D41738F7EDDF3A
Refresh timer is set for 00:01:24
```

show cts role-based counters

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

show cts role-based counters { **default** | { **ipv4** | **ipv6** } } { { [**from** | [*sgt_number* | **unknown**] | { **ipv4** | **ipv6** | **to** | [*sgt_number* | **unknown**] | { **ipv4** | **ipv6** } }] } } { **to** | [*sgt_number* | **unknown**] | { **ipv4** | **ipv6** } } { **ipv4** | **ipv6** }

Syntax Description

default	Specifies default policy counters.
from	Specifies the source security group.
ipv4	Specifies security groups on IPv4 networks.
ipv6	Specifies security groups on IPv6 networks.
to	Specifies the destination security group.
sgt_num	Security Group Tag number. Valid values are from 0 to 65533.
unknown	Specifies all source groups.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	This command was introduced.

Usage Guidelines

Use the **show cts role-based counters** command to display the Security Group ACL (SGACL) enforcement statistics. Use the **clear cts role-based counters** to reset all or a range of statistics.

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

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

Examples

The following sample output displays all enforcement statistics for IPv4 and IPv6 events:

```
Device# show cts role-based counters

 Role-based counters

From To SW-Denied HW-Denied SW-Permitted HW_Permitted
2 5 129 89762 421 7564328
3 5 37 123456 1325 12345678
3 7 0 65432 325 2345678
```

show cts role-based permissions

To display the Cisco TrustSec role-based access control list (RBACL) permissions, use the **show cts role-based permissions** command in privileged EXEC mode.

show cts role-based permissions { { **default** } | { **from** } | { **ipv4** } | { **ipv6** } | { **to** } } { **details** }

show cts role-based permissions { { **default** } | { **from** } | { **ipv4** } | { **to** } } { **details** }

Syntax Description

default	(Optional) Displays the default permission list.
from	(Optional) Displays the source group.
ipv4	(Optional) Displays the IPv4 RBACLs.
ipv6	(Optional) Displays the IPv6 RBACLs.
to	(Optional) Displays the destination group.
details	(Optional) Displays the attached access control list (ACL) details.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	This command was introduced.

Usage Guidelines

This show command displays the content of the RBACL permission matrix. You can specify the source SGT by using the **from** keyword and the destination SGT by using the **to** keyword. When both **from** and **to** are specified the RBACLs of a single cell are displayed. An entire column is displayed when only the **to** is used. An entire row is displayed when the **from** keyword is used.

The entire permission matrix is displayed when both the **from** clause and **to** keywords are omitted.

The command output is sorted by destination SGT as a primary key and the source SGT as a secondary key. The RBACLs for each cell is displayed in the same order they are defined in the configuration or acquired from Cisco ACS.

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 ACEs of the RBACLs of a single cell are displayed.

Examples

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

```
Device# show cts role-based permissions

 Role-based permissions from group 2 to group 5:
srb2
srb5
Role-based permissions from group 3 to group 5:
srb3
srb5
Role-based permissions from group 3 to group 7:
srb4
```

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

```
Device# show cts role-based permissions

 Role-based permissions from group 2 to group 5:
srb2
srb5
```

show cts role-based sgt-map

To display the Security Group Tag (SGT) Exchange Protocol (SXP) source IP-to-SGT bindings table, use the **show cts role-based sgt-map** command in user EXEC or privileged EXEC mode.

show cts role-based sgt-map [*ipv4_dec ipv4_cidr ipv6_hex ipv6_cidr* | **all** | { **ipv4** | **ipv6** } | **host** | [*ipv4_decimal ipv6_dec*] | **summary** | { **ipv4** | **ipv6** } | **vrf** *instance_name* | [*ipv4_dec ipv4_cidr ipv6_dec ipv6_cidr* | **all** | [**ipv4** | **ipv6**] | **host** | [*ipv4_decimal ipv6_dec*] | **summary** | [**ipv4** | **ipv6**]]]

Syntax Description

ipv4_dec	IPv4 address in dot-decimal notation. For example (208.77.188.166)
ipv4_cidr	IPv4 address range in Classless Inter-Domain Routing (CIDR) For example, 10.0.0.0/8, where the /8 signifies that the 8 most significant bits identify the networks, and the 24 least-significant bits, the hosts.
ipv6_hex	IPv6 address in hexadecimal separated by colons. For example, 2001:db8:85a3::8a2e:370:7334.
ipv6_cidr	A range of IPv6 address in hexadecimal CIDR notation.
host*ipv4_decimalipv6_hex*	Specifies mappings for a specific IPv4 or IPv6 host. Use dot decimal and hex colon notation for IPv4 and IPv6 respectively.
all	Specifies all mappings to be displayed.
summary*ipv4ipv6*	Summary of IPv4 or IPv6 mappings. Displays both IPv4 and IPv6 if you do not specify a keyword.
vrf*instance_name*	Specifies a VPN routing and forwarding instance for mappings.

Command Default

None

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	This command was introduced.

Usage Guidelines

Use this command to verify that source IP addresses to the appropriate Security Group Tags bindings are correct. This command shows information about active IP-SGT bindings for the specified IP host address or subnet.

This command displays a single binding when host IP address is specified. It displays all the bindings for IP addresses within a given subnet if <network>/<length> is specified.

A summary of the active bindings by source is displayed at the end of the keyword all output and also if the keyword summary is entered.

Examples

The following sample output displays the bindings of IP address and SGT source names:

```
Device# show cts role-based sgt-map vrf 1 all

Active IPv4-SGT Bindings Information
IP Address SGT Source
============================================
10.1.1.1 500 CLI
10.2.2.2 600 SXP
IP-SGT Active Bindings Summary
============================================
Total number of CLI bindings = 1
Total number of SXP bindings = 1
Total number of active bindings = 2
```

show cts sxp connections

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

Supported Parameters

connections	Displays Cisco TrustSec SXP connections information.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	This command was introduced.

Usage Guidelines

For more information about this command, see the Cisco IOS XE show cts sxp

Examples

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

```
Device# show cts sxp connection brief

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

The following example displays the CTS-SXP connections:

```
Device# show cts sxp connections

 SXP              : Enabled
 Default Password : Set
 Default Source IP: Not Set
Connection retry open period: 10 secs
Reconcile period: 120 secs
Retry open timer is not running
------------------------------------------------
Peer IP          : 10.10.10.1
Source IP        : 10.10.10.2
Set up           : Peer
Conn status      : On
Connection mode  : SXP Listener
Connection inst# : 1
TCP conn fd      : 1
TCP conn password: not set (using default SXP password)
Duration since last state change: 0:00:01:25 (dd:hr:mm:sec)
------------------------------------------------
Peer IP          : 10.10.2.1
Source IP        : 10.10.2.2
Set up           : Peer
Conn status      : On
Connection mode  : SXP Listener
TCP conn fd      : 2
TCP conn password: not set (using default SXP password)
Duration since last state change: 0:00:01:25 (dd:hr:mm:sec)
Total num of SXP Connections = 2
```

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

```
Device# show cts sxp connections

SXP : Enabled
Highest Version Supported: 4
Default Password : Set
Default Source IP: Not Set
```

```
Connection retry open period: 120 secs
Reconcile period: 120 secs
Retry open timer is running
----------------------------------------------
Peer IP : 2.0.0.2
Source IP : 1.0.0.2
Conn status : On (Speaker) :: On (Listener)
Conn version : 4
Local mode : Both
Connection inst# : 1
TCP conn fd : 1(Speaker) 3(Listener)
TCP conn password: default SXP password
Duration since last state change: 1:03:38:03 (dd:hr:mm:sec) :: 0:00:00:46 (dd:hr:mm:sec)
```

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

```
Device# show cts sxp connections

 SXP              : Enabled
 Default Password : Set
 Default Source IP: Not Set
Connection retry open period: 10 secs
Reconcile period: 120 secs
Retry open timer is not running
----------------------------------------------
Peer IP          : 10.10.10.1
Source IP        : 10.10.10.2
Set up           : Peer
Conn status      : Delete_Hold_Down
Connection mode  : SXP Listener
Connection inst# : 1
TCP conn fd      : -1
TCP conn password: not set (using default SXP password)
Delete hold down timer is running
Duration since last state change: 0:00:00:16 (dd:hr:mm:sec)
----------------------------------------------
Peer IP          : 10.10.2.1
Source IP        : 10.10.2.2
Set up           : Peer
Conn status      : On
Connection inst# : 1
TCP conn fd      : 2
TCP conn password: not set (using default SXP password)
Duration since last state change: 0:00:05:49 (dd:hr:mm:sec)
Total num of SXP Connections = 2
```

show crypto key mypubkey rsa

To display the RSA public keys of your router, use the **show crypto key mypubkey rsa** command in privileged EXEC mode.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For more information about this command, see the Cisco IOS XE show crypto key mypubkey rsa command.

The following example shows the status information for all active crypto sessions:

```
Device#show crypto key mypubkey rsa
Key name: TRUST_POINT_100
Key type: RSA KEYS
 Storage Device: private-config
 Usage: General Purpose Key
 Key is not exportable. Redundancy enabled.
 Key Data:
  30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
  00B4E83F ABAE87DC DB7ACBB2 844F5FD6 FF2E9E02 DE49A302 D3D7884F 0B26EE6A
  D3D56275 4D733A4F 5D974061 CE8FB520 54276D6D 3B132C82 EB8A3C24 115F77F5
  C38740CE 1BBD89DB 3F766728 649B63FC 2C40C3AD 251656A1 BAF8341E 1736F03D
  0A0D15AF 0E9D3E94 4E2074C7 BA572CA3 95B3D664 916ADA74 281CDE07 B3DD0B42
  13289610 32E611AB 2B3B4EB6 0A3573B1 F097AC2A 3720961C 97597201 3CE8171C
  F02B99B4 3B7B718F 83E221E1 E172554D C2BEA127 93882766 A28C5E8C 4B83BDC5
  A161597D 2C3D8E13 3BE00D8F 02D0AD55 962DF402 599580A6 F049DBF4 045D751B
  A8932156 10B29D9F 037AB33F C1FC463D E59E014C 27660223 546A8B3A E6997713
  CF020301 0001
% Key pair was generated at: 00:22:51 UTC Oct 27 2021
```

show crypto ikev2 stats

To display the IKEv2 statistics, use the **show crypto ikev2 stats** command in privileged EXEC mode.

show crypto ikev2 stats

Command Default

The command has no default.

Command Modes

Priviledged EXEC

Example

The command output shows the IKEv2 statistics. The "Max in nego" portion shows the maximum in negotiation, incoming and outgoing, which means the maximum number of incoming and outgoing connections the device supports.

```
sdwan-manager#show crypto ikev2 stats
                     Crypto IKEv2 SA Statistics
System Resource Limit:   0        Max IKEv2 SAs: 0        Max in nego(in/out): 40/400
Total incoming IKEv2 SA Count:    0        active:        0        negotiating: 0
Total outgoing IKEv2 SA Count:    0        active:        0        negotiating: 0
Incoming IKEv2 Requests: 0        accepted:      0        rejected:    0
Outgoing IKEv2 Requests: 0        accepted:      0        rejected:    0
Rejected IKEv2 Requests: 0        rsrc low:      0        SA limit:    0
IKEv2 packets dropped at dispatch: 0
Incoming Requests dropped as LOW Q limit reached : 0
Incoming IKEV2 Cookie Challenged Requests: 0
```

```
accepted: 0        rejected: 0        rejected no cookie: 0
Total Deleted sessions of Cert Revoked Peers: 0
Total init sa request rejected due to queue limit : 0
SA Strength Enforcement Rejects - incoming:        0 outgoing:        0
Sessions with Quantum Resistance: 0        Manual: 0        Dynamic: 0
PPK Identity Mismatch: 0
PPK Retrieve Failure    -    ALL:      0        With PPK Required:    0
PPK Authentication Failure - ALL:      0        With PPK Required:    0
```

Related commands

Command	Description
crypto ikev2 limit	Configures the maximum number of active incoming or outgoing connections from a device.

show crypto pki certificates

To display information about your certificate, the certification authority certificate (CA), and any registration authority (RA) certificates, use the **show crypto pki certificates** command in privileged EXEC mode.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For more information about this command, see the Cisco IOS XE show crypto pki certificates command

The following is sample output from the **show crypto pki certificates** command after you authenticated the CA by requesting the certificate of the CA and public key with the crypto pki authenticate command.

```
Device#show crypto pki certificates
CA Certificate
  Status: Available
  Certificate Serial Number: 3051DF7123BEE31B8341DFE4B3A338E5F
  Key Usage: Not Set
```

The CA certificate might show Key Usage as "Not Set."

The following is sample output from the **show crypto pki certificates** command, and it shows the certificate of the router and the certificate of the CA. In this example, a single, general-purpose Rivest, Shamir, and Adelman (RSA) key pair was previously generated, and a certificate was requested but not received for that key pair.

```
Device#show crypto pki certificates
Certificate
  Subject Name
    Name: myrouter.example.com
    IP Address: 10.0.0.1
    Serial Number: 04806682
  Status: Pending
  Key Usage: General Purpose
    Fingerprint: 428125BD A3419600 3F6C7831 6CD8FA95 00000000
```

```
CA Certificate
  Status: Available
  Certificate Serial Number: 3051DF7123BEE31B8341DFE4B3A338E5F
  Key Usage: Not Set
```

Note In the previous sample, the certificate status of the device shows "Pending." After the device receives its certificate from the CA, the Status field changes to "Available" in the show output.

The following is sample output from the **show crypto pki certificates** command, and it shows the certificates of two routers and the certificate of the CA. In this example, special-usage RSA key pairs were previously generated, and a certificate was requested and received for each key pair.

```
Device#show crypto pki certificates
Certificate
  Subject Name
    Name: myrouter.example.com
    IP Address: 10.0.0.1
  Status: Available
  Certificate Serial Number: 428125BDA34196003F6C78316CD8FA95
  Key Usage: Signature

Certificate
  Subject Name
    Name: myrouter.example.com
    IP Address: 10.0.0.1
  Status: Available
  Certificate Serial Number: AB352356AFCD0395E333CCFD7CD33897
  Key Usage: Encryption

CA Certificate
  Status: Available
  Certificate Serial Number: 3051DF7123BEE31B8341DFE4B3A338E5F
  Key Usage: Not Set
```

The following is sample output from the **show crypto pki certificates** command when the CA supports an RA. In this example, the CA and RA certificates were previously requested with the **crypto pki authenticate** command.

```
Device#show crypto pki certificates
CA Certificate
  Status: Available
  Certificate Serial Number: 3051DF7123BEE31B8341DFE4B3A338E5F
  Key Usage: Not Set
RA Signature Certificate
  Status: Available
  Certificate Serial Number: 34BCF8A0
  Key Usage: Signature

RA KeyEncipher Certificate
  Status: Available
  Certificate Serial Number: 34BCF89F
  Key Usage: Encryption
```

The following is sample output from the **show crypto pki certificates** using the optional trustpoint-name argument and verbose keyword. The output shows the certificate of a router and the

certificate of the CA. In this example, general-purpose RSA key pairs were previously generated, and a certificate was requested and received for the key pair.

```
Device#show crypto pki certificates verbose TRUST_POINT_100
Certificate
  Status: Available
  Version: 3
  Certificate Serial Number (hex): 31
  Certificate Usage: General Purpose
  Issuer:
    o=CRDC
    ou=CRDC-Lab
    cn=vCisco-CA
  Subject:
    Name: ROUTER1
    cn=ROUTER1
    o=Internet Widgits Pty Ltd
    st=Some-State
    c=AU
  Validity Date:
    start date: 12:57:14 UTC Jul 24 2021
    end   date: 12:57:14 UTC Jul 22 2031
  Subject Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (2048 bit)
  Signature Algorithm: SHA1 with RSA Encryption
  Fingerprint MD5: D0AD3252 586C0DB8 9F4EFC15 1D81AC5F
  Fingerprint SHA1: 6824ED1A C1405149 577CF210 C0BC83D1 8741F0D1
  X509v3 extensions:
    X509v3 Subject Key ID: E806DCF5 89698C43 97795999 4440D7F1 16F9827C
    X509v3 Authority Key ID: 91C2776C 651DF253 08FA9614 D2082F99 BEBF0B00
    Authority Info Access:
  Cert install time: 08:29:26 UTC Oct 21 2021
  Associated Trustpoints: TRUST_POINT_100
  Storage: nvram:CRDC#31.cer
  Key Label: TRUST_POINT_100
  Key storage device: private config

CA Certificate
  Status: Available
  Version: 3
  Certificate Serial Number (hex): 01
  Certificate Usage: Signature
  Issuer:
    o=CRDC
    ou=CRDC-Lab
    cn=vCisco-CA
  Subject:
    o=CRDC
    ou=CRDC-Lab
    cn=vCisco-CA
  Validity Date:
    start date: 13:41:14 UTC Feb 9 2018
    end   date: 13:41:14 UTC Feb 9 2038
  Subject Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (4096 bit)
  Signature Algorithm: SHA1 with RSA Encryption
  Fingerprint MD5: 5ECA97DB 97FF1B95 DFEEB8FB DAB6656F
  Fingerprint SHA1: 73A7E91E 3AB12ABE 746348E4 A0E21BE3 8413130C
  X509v3 extensions:
    X509v3 Key Usage: 86000000
      Digital Signature
      Key Cert Sign
```

```
    CRL Signature
  X509v3 Subject Key ID: 91C2776C 651DF253 08FA9614 D2082F99 BEBF0B00
  X509v3 Basic Constraints:
      CA: TRUE
  X509v3 Authority Key ID: 91C2776C 651DF253 08FA9614 D2082F99 BEBF0B00
  Authority Info Access:
Cert install time: 08:29:23 UTC Oct 21 2021
Associated Trustpoints: TRUST_POINT_ex TRUST_POINT_100
Storage: nvram:CRDC#1CA.cer
```

show crypto session

To display status information for active crypto sessions, use the **show crypto session** command in privileged EXEC mode.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For more information about this command, see the Cisco IOS XE show crypto session command.

The following example shows the status information for all active crypto sessions:

```
Device#show crypto session
Crypto session current status
Interface: Virtual-Access2
Username: cisco
Profile: prof
Group: easy
Assigned address: 10.3.3.4
Session status: UP-ACTIVE
Peer: 10.1.1.2 port 500
  IKE SA: local 10.1.1.1/500 remote 10.1.1.2/500 Active
  IKE SA: local 10.1.1.1/500 remote 10.1.1.2/500 Inactive
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 host 3.3.3.4
        Active SAs: 2, origin: crypto map
```

The following example shows the show crypto session detail command output.

```
Device#show crypto session detail
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation
R - IKE Auto Reconnect, U - IKE Dynamic Route Update
S - SIP VPN

Interface: Tunnel100
Profile: cisco
Uptime: 03:59:01
Session status: UP-ACTIVE
Peer: 10.0.21.16 port 500 fvrf: (none) ivrf: 11
      Phase1_id: cn=ROUTER2,o=Internet Widgits Pty Ltd,st=Some-State,c=AU
      Desc: (none)
  Session ID: 1780
```

```
IKEv2 SA: local 10.0.20.15/500 remote 10.0.21.16/500 Active
        Capabilities:U connid:1 lifetime:20:00:59
IPSEC FLOW: permit 47 host 10.0.20.15 host 10.0.21.16
      Active SAs: 2, origin: crypto map
      Inbound:  #pkts dec'ed 1668 drop 0 life (KB/Sec) KB Vol Rekey Disabled/2294
      Outbound: #pkts enc'ed 1665 drop 0 life (KB/Sec) KB Vol Rekey Disabled/2294
```

show endpoint-tracker

To display individual tracker status, tracker group status, and tracker group configurations, use the **show endpoint-tracker** command in privileged EXEC mode.

show endpoint-tracker [**interface** *interface-type/number* | **records** | **static-route** | **tracker-group** | **sla-profile** | **sla-mode** | **sla-status** | **sla-statistics** | **history**]

Syntax Description

interface	Shows the endpoint tracker information on one interface.
records	Shows the endpoint tracker records.
static-route	Shows the static-route endpoint trackers.
tracker-group	Shows the endpoint tracker group.
sla-profile	Shows the endpoint tracker sla-profile.
sla-mode	Shows all the available SLA modes and the associated parameter values.
sla-status	Shows the endpoint tracker sla-status.
sla-statistics	Shows the endpoint tracker sla-statistics.
history	Shows the endpoint-tracker history including information when there is no connection.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.
Cisco IOS XE Catalyst SD-WAN Release 17.14.1a	Added the following keywords: sla-profile, sla-mode, sla-status, and sla-statistics
Cisco IOS XE Catalyst SD-WAN Release 17.18.1a	Added the following keyword: history

Examples

The following is a sample output from the **show endpoint-tracker static-route** command:

```
Device# show endpoint-tracker static-route
Tracker Name      Status   RTT in msec     Probe ID
vm7-tcp-10001     UP           3               1
vm7-tcp-10002     UP           2               2
vm7-tcp-10003     UP           5               3
```

```
vm7-tcp-10004     UP           5               4
vm7-udp-10001     UP           1               5
vm7-udp-10002     UP           1               6
vm7-udp-10003     UP           1               7
vm7-udp-10004     UP           1               8
```

The following is a sample output from the **show endpoint-tracker tracker-group** command:

```
Device# show endpoint-tracker tracker-group
Tracker Name                    Element trackers name            Status          RTT in
msec   Probe ID
vm7-group-tcp-10001-udp-10002    vm7-tcp-10001, vm7-udp-10002     UP(UP AND UP)   5, 1
      9, 10
vm7-group-tcp-10003-udp-10004    vm7-tcp-10003, vm7-udp-10004     UP(UP AND UP)   5, 1
      13, 14
vm7-group-udp-10001-tcp-10002    vm7-tcp-10002, vm7-udp-10001     UP(UP OR UP)    4, 1
      11, 12
vm7-group-udp-10003-tcp-10004    vm7-tcp-10004, vm7-udp-10003     UP(UP OR UP)    4, 1
      15, 16
interface-tracker-group          tracker1, tracker2               UP(UP OR UP)    1,1
      53, 54
```

The following is a sample output from the **show endpoint-tracker records** command:

```
Device# show endpoint-tracker records
Record Name                    Endpoint                         EndPoint Type Threshold(ms)
 Multiplier Interval(s) Tracker-Type
vm7-group-tcp-10001-udp-10002    vm7-tcp-10001 AND vm7-udp-10002      N/A           N/A
        N/A        N/A      tracker-group
vm7-group-tcp-10003-udp-10004    vm7-tcp-10003 AND vm7-udp-10004      N/A           N/A
        N/A        N/A      tracker-group
vm7-group-udp-10001-tcp-10002    vm7-tcp-10002 OR vm7-udp-10001       N/A           N/A
        N/A        N/A      tracker-group
vm7-group-udp-10003-tcp-10004    vm7-tcp-10004 OR vm7-udp-10003       N/A           N/A
        N/A        N/A      tracker-group
vm7-tcp-10001                    10.0.0.1                             TCP           100
        1          20       static-route
vm7-tcp-10002                    10.0.0.2                             TCP           100
        1          20       static-route
vm7-udp-10001                    10.0.0.1                             UDP           100
        1          20       static-route
vm7-udp-10002                    10.0.0.2                             UDP           100
        1          20       static-route
group1                           tracker1 OR tracker2                 N/A           N/A
        N/A        N/A      tracker-group
group3                           tracker3 OR tracker4                 N/A           N/A
        N/A        N/A      tracker-group
tracker1                         198.168.20.2                         IP            300
        3          60       interface
tracker2                         198.168.20.3                         IP            300
        3          60       interface
tracker3                         www.diatracker.com                   DNS_NAME      300
        3          60       interface
tracker4                         www.newdiatracker.com                DNS_NAME      300
        3          60       interface
```

The following is a sample output from the **show endpoint-tracker interface** command:

```
Device# show endpoint-tracker interface GigabitEthernet1
Interface      Record Name     Status   RTT in msecs  Probe ID    Next Hop
track-static              1:172.16.1.2    UP        2             11        10.1.1.1
track-static-ro           DIA-Tracker     UP        8             21        172.16.11.1
track-static_static-ro    track-static    UP        1             9         10.1.1.1
GigabitEthernet1          tracker-t1      UP        2             1         10.1.16.13
```

The following is a sample output from the **show endpoint-tracker sla-mode** command:

```
Device# show endpoint-tracker sla-mode
SLA mode             Poll Interval(Secs)  Poll multiplier(buckets)     Dampening multiplier
      Dampening window(Secs)

=============================================================================================
Aggressive           60                   1                            1
       60
Moderate             120                  1                            2
       240
Conservative         300                  1                            3
       900
```

The following is a sample output from the **show endpoint-tracker history** command:

```
Device# show endpoint-tracker history
Legend:
INVALID - Invalid Tracker State
DNS_CFG_ERR - Error configuring DNS probe
DNS_SCHEDULED_ERR - Error scheduling DNS probe
DNS_INPRGRS - DNS probe is in progress
DNS_SUCCESS - DNS resolution is successful
DNS_ERR - DNS resolution failed
PRB_EP_RSLVD - Probe endpoint is resolved
PRB_CFG_ERR - Error configuring tracker probe
PRB_SCHEDULED_ERR - Error scheduling tracker probe
PRB_INPRGRS - Tracker probe is in progress
PRB_ERR - Probe Error


Timestamp            | Attach Point                    | Tracker Name           | Tracker
 Status   | Latency            | Resolved Endpoint  | Next Hop        | Tracker State   |
DNS State       | Probe ID        | DNS Probe ID
=============================================================================================
2025-01-29T05:30:03  | GigabitEthernet1                | test-track1            | Up
          | 2                  | 142.251.32.45      | 10.0.29.26      | PRB_EP_RSLVD    |
DNS_SUCCESS     | 15               | 14
2025-01-29T05:29:05  | GigabitEthernet1                | test-track1            | Up
          | Timeout            | 142.251.32.45      | 10.0.29.26      | PRB_EP_RSLVD    |
DNS_SUCCESS     | 15               | 14
2025-01-29T05:17:03  | GigabitEthernet1                | test-track1            | Up
          | 1                  | 142.251.32.45      | 10.0.29.26      | PRB_EP_RSLVD    |
DNS_SUCCESS     | 15               | 14
2025-01-29T05:16:05  | GigabitEthernet1                | test-track1            | Up
          | Timeout            | 142.251.32.45      | 10.0.29.26      | PRB_EP_RSLVD    |
DNS_SUCCESS     | 15               | 14
2025-01-29T05:08:03  | GigabitEthernet1                | test-track1            | Up
          | 1                  | 142.251.32.45      | 10.0.29.26      | PRB_EP_RSLVD    |
DNS_SUCCESS     | 15               | 14
2025-01-29T05:07:08  | GigabitEthernet1                | test-track1            | Up
          | Timeout            | 142.251.32.45      | 10.0.29.26      | PRB_EP_RSLVD    |
DNS_SUCCESS     | 15               | 14
2025-01-29T05:00:03  | GigabitEthernet1                | test-track1            | Up
          | 1                  | 142.251.32.45      | 10.0.29.26      | PRB_EP_RSLVD    |
DNS_SUCCESS     | 15               | 14
2025-01-29T04:59:05  | GigabitEthernet1                | test-track1            | Up
          | Timeout            | 142.251.32.45      | 10.0.29.26      | PRB_EP_RSLVD    |
DNS_SUCCESS     | 15               | 14
2025-01-29T01:22:03  | GigabitEthernet1                | test-track1            | Up
          | 1                  | 142.251.32.45      | 10.0.29.26      | PRB_EP_RSLVD    |
DNS_SUCCESS     | 15               | 14
2025-01-29T01:21:08  | GigabitEthernet1                | test-track1            | Up
          | Timeout            | 142.251.32.45      | 10.0.29.26      | PRB_EP_RSLVD    |
DNS_SUCCESS     | 15               | 14
```

The following table below describes the significant fields shown in the sample output.

Table 76: show endpoint-tracker command Field Descriptions

Field	Description
Tracker Name	Displays names of the configured trackers.
Status	Displays the UP or DOWN status of the trackers, tracker group, and interfaces.
RTT in msecs	Displays the round-trip time of a tracker during which packets are sent to an endpoint and a response is received in ms. RTT includes total time of latest DNS RTT, latest TCP connection RTT and latest HTTP transaction RTT. **Note** For Viptela OS, latency is half of RTT value. For each transaction timer reset, if threshold value is set to RTT value seen, which is always equal to twice the latency, timer never expires, and tracker status is always up, even if the latency exceeds.
Probe ID	Displays the IDs assigned to each active tracker. Two probe IDs are displayed for a tracker group, and one probe ID is displayed for an individual tracker.
Element Tracker Name	Displays the tracker names associated with the tracker group.
Record Name	Displays all the configured trackers or tracker group names.
Endpoint	Displays all the configured endpoints. Two types of endpoint trackers are supported—static-route tracker and interface tracker.
Endpoint Type	Displays the endpoint types configurations—IP address, DNS name, API URL, TCP/UDP.
Threshold (ms)	Displays wait time for the probe to return a response before declaring that the configured endpoint is down.
Multiplier	Displays the number of times probes are sent to the endpoints.
Interval (s)	Displays the time interval between which probes are sent to the endpoints.
Tracker Type	Displays the tracker type configured. Supported types are interface, static-route, and tracker-group.
Interface	Displays endpoint-tracker information for the specified interface.
Next Hop	Displays IPv4 addresses of the next hop.

show etherchannel load-balancing

To display information about EtherChannel load balancing, use the **show etherchannel load-balancing** command in privileged EXEC mode.

show etherchannel load-balancing

Command Default None

Command Modes Privileged EXEC (#))

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	This command was introduced.

Examples The following sample output displays information about EtherChannel load balancing.

```
Device# show etherchannel load-balancing
EtherChannel Load-Balancing Method:
Global LB Method: vlan-manual

  Port-Channel:                       LB Method
    Port-channel1                   :  flow-based
```

show etherchannel summary

To display EtherChannel information, use the **show etherchannel summary** command in privileged EXEC mode.

show etherchannel summary

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	This command was introduced.

Examples The following sample output displays the EtherChannel information.

```
Device# show etherchannel summary
Flags:  D - down        P/bndl - bundled in port-channel
        I - stand-alone s/susp - suspended
```

```
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


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

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1       Po1(RU)         LACP     Te0/3/0(bndl) Te0/3/1(hot-sby)

RU - L3 port-channel UP State
SU - L2 port-channel UP state
P/bndl -  Bundled
S/susp  - Suspended
```

show flow exporter

To view flow exporter status and statistics, use the **show flow exporter** command in privileged EXEC mode.

show flow exporter [*exporter-name*] [**templates**]

Syntax Description

exporter-name	(Optional) Name of a flow exporter that was previously configured.
templates	(Optional) Displays flow exporter template information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	This command can be used in controller mode to view flow exporter statistics for Cisco SD-WAN performance monitor.

The following is sample output from the **show flow exporter** command. The output displays the template format for exporters that are configured on the device. This output varies according to the flow record configured:

```
Device# show flow exporter CISCO-MONITOR templates

Flow Exporter CISCO-MONITOR:

  Client: Option options interface-table

  Exporter Format: IPFIX (Version 10)
```

```
Template ID    : 256
Source ID      : 6
Record Size    : 102
Template layout
```

Field	ID	Ent.ID	Offset	Size
INTERFACE INPUT SNMP	10		0	4
interface name short	82		4	33
interface name long	83		37	65

```
Client: Option options sampler-table
Exporter Format: IPFIX (Version 10)
Template ID    : 257
Source ID      : 6
Record Size    : 48
Template layout
```

Field	ID	Ent.ID	Offset	Size
FLOW SAMPLER	48		0	4
flow sampler name	84		4	41
flow sampler algorithm export	49		45	1
flow sampler interval	50		46	2

```
Client: Option options application-name
Exporter Format: IPFIX (Version 10)
Template ID    : 258
Source ID      : 6
Record Size    : 83
```

```
Template layout
_______________________________________________________________________________
|                 Field                   |    ID | Ent.ID | Offset |  Size |
-------------------------------------------------------------------------------
| APPLICATION ID                          |    95 |        |      0 |     4 |
| application name                        |    96 |        |      4 |    24 |
| application description                 |    94 |        |     28 |    55 |
-------------------------------------------------------------------------------

Client: Option sub-application-table
Exporter Format: IPFIX (Version 10)
Template ID    : 259
Source ID      : 6
Record Size    : 168
Template layout
_______________________________________________________________________________
|                 Field                   |    ID | Ent.ID | Offset |  Size |
-------------------------------------------------------------------------------
| APPLICATION ID                          |    95 |        |      0 |     4 |
| SUB APPLICATION TAG                     |    97 |        |      4 |     4 |
| sub application name                    |   109 |        |      8 |    80 |
| sub application description             |   110 |        |     88 |    80 |
-------------------------------------------------------------------------------

Client: Option options application-attributes
Exporter Format: IPFIX (Version 10)
Template ID    : 260
Source ID      : 6
Record Size    : 258
Template layout
_______________________________________________________________________________
|                 Field                   |    ID | Ent.ID | Offset |  Size |
-------------------------------------------------------------------------------
```

```
| APPLICATION ID                          |    95 |        |      0 |     4 |

| application category name               | 12232 |      9 |      4 |    32 |

| application sub category name           | 12233 |      9 |     36 |    32 |
| application group name                  | 12234 |      9 |     68 |    32 |

| application traffic-class               | 12243 |      9 |    100 |    32 |

| application business-relevance          | 12244 |      9 |    132 |    32 |

| p2p technology                          |   288 |        |    164 |    10 |

| tunnel technology                       |   289 |        |    174 |    10 |

| encrypted technology                    |   290 |        |    184 |    10 |

| application set name                    | 12231 |      9 |    194 |    32 |

| application family name                 | 12230 |      9 |    226 |    32 |

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


  Client: Option options tunnel-tloc-table

  Exporter Format: IPFIX (Version 10)

  Template ID    : 261

  Source ID      : 6

  Record Size    : 52

  Template layout

_______________________________________________________________________________

|                Field                    |    ID | Ent.ID | Offset |  Size |

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

| TLOC TABLE OVERLAY SESSION ID           | 12435 |      9 |      0 |     4 |

| tloc local color                        | 12437 |      9 |      4 |    16 |

| tloc remote color                       | 12439 |      9 |     20 |    16 |

| tloc tunnel protocol                    | 12440 |      9 |     36 |     8 |

| tloc local system ip address            | 12436 |      9 |     44 |     4 |

| tloc remote system ip address           | 12438 |      9 |     48 |     4 |

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


Client: Flow Monitor CISCO-MONITOR-art_ipv4

  Exporter Format: IPFIX (Version 10)
```

```
Template ID    : 0

Source ID      : 0

Record Size    : 208

Template layout
```

Field	ID	Ent.ID	Offset	Size
interface input snmp	10		0	4
connection client ipv4 address	12236	9	4	4
connection server ipv4 address	12237	9	8	4
ip dscp	195		12	1
ip protocol	4		13	1
ip ttl	192		14	1
connection server transport port	12241	9	15	2
connection initiator	239		17	1
timestamp absolute monitoring-interval	359		18	8
flow observation point	138		26	8
overlay session id input	12432	9	34	4
routing vrf service	12434	9	38	4
application id	95		42	4
interface output snmp	14		46	4
flow direction	61		50	1
flow sampler	48		51	1
overlay session id output	12433	9	52	4
timestamp absolute first	152		56	8
timestamp absolute last	153		64	8
connection new-connections	278		72	4
connection sum-duration	279		76	8
connection server counter bytes long	232		84	8
connection server counter packets long	299		92	8
connection client counter bytes long	231		100	8
connection client counter packets long	298		108	8
connection server counter bytes network	8337	9	116	8

```
  | connection client counter bytes network |  8338 |      9 |    124 |      8 |
  | connection delay response to-server sum |  9303 |      9 |    132 |      4 |
  | connection server counter responses     |  9292 |      9 |    136 |      4 |
  | connection delay response to-server his |  9300 |      9 |    140 |      4 |
  | connection client counter packets retra |  9268 |      9 |    144 |      4 |
  | connection delay application sum        |  9306 |      9 |    148 |      4 |
  | connection delay response client-to-ser |  9309 |      9 |    152 |      4 |
  | connection transaction duration sum     |  9273 |      9 |    156 |      4 |
  | connection transaction duration min     |  9275 |      9 |    160 |      4 |
  | connection transaction duration max     |  9274 |      9 |    164 |      4 |
  | connection transaction counter complete |  9272 |      9 |    168 |      4 |
  | connection client counter bytes retrans |  9267 |      9 |    172 |      4 |
  | connection server counter bytes retrans |  9269 |      9 |    176 |      4 |
  | connection server counter packets retra |  9270 |      9 |    180 |      4 |
  | connection delay network long-lived to- |  9255 |      9 |    184 |      4 |
  | connection delay network to-client num- |  9259 |      9 |    188 |      4 |
  | connection delay network long-lived to- |  9254 |      9 |    192 |      4 |
  | connection delay network to-server num- |  9258 |      9 |    196 |      4 |
  | connection delay network long-lived cli |  9256 |      9 |    200 |      4 |
  | connection delay network client-to-serv |  9257 |      9 |    204 |      4 |
  ------------------------------------------------------------------------------


Client: Flow Monitor CISCO-MONITOR-media_ipv4
  Exporter Format: IPFIX (Version 10)
  Template ID    : 0
  Source ID      : 0
  Record Size    : 180
  Template layout
  ______________________________________________________________________________
  |                 Field                   |    ID | Ent.ID | Offset |  Size |
  ------------------------------------------------------------------------------
  | ipv4 source address                     |     8 |        |      0 |     4 |
```

ipv4 destination address	12		4	4
interface input snmp	10		8	4
ip dscp	195		12	1
ip protocol	4		13	1
ip ttl	192		14	1
ipv6 source address	27		15	16
ipv6 destination address	28		31	16
transport source-port	7		47	2
transport destination-port	11		49	2
connection initiator	239		51	1
timestamp absolute monitoring-interval	359		52	8
flow observation point	138		60	8
overlay session id input	12432	9	68	4
routing vrf service	12434	9	72	4
application id	95		76	4
routing forwarding-status	89		80	1
interface output snmp	14		81	4
flow direction	61		85	1
flow sampler	48		86	1
overlay session id output	12433	9	87	4
transport rtp ssrc	4254	9	91	4
transport rtp payload-type	4273	9	95	1
counter bytes long	1		96	8
counter packets	2		104	4
timestamp absolute first	152		108	8
timestamp absolute last	153		116	8
connection new-connections	278		124	4
transport packets expected counter	4246	9	128	4
transport packets lost counter	4251	9	132	4
transport packets lost rate	4253	9	136	4
transport rtp jitter mean	4255	9	140	4
transport rtp jitter minimum	4256	9	144	4
transport rtp jitter maximum	4257	9	148	4

```
| counter bytes rate                      |  4235 |      9 |    152 |      4 |
| application media bytes counter         |  4236 |      9 |    156 |      4 |
| application media bytes rate            |  4238 |      9 |    160 |      4 |
| application media packets counter       |  4239 |      9 |    164 |      4 |
| application media packets rate          |  4241 |      9 |    168 |      4 |
| transport rtp jitter mean sum           |  4325 |      9 |    172 |      8 |
--------------------------------------------------------------------------------
```

show flow monitor sdwan_flow_monitor cache

To ensure that Unified Logging is enabled successfully for security connection events, use the **show flow monitor sdwan_flow_monitor cache** command in privileged EXEC mode.

show flow monitor sdwan_flow_monitor cache

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

The following is sample output from the **show flow monitor sdwan_flow_monitor cache** command that displays Unified Logging status for the security connection events:

```
IPV4 SOURCE ADDRESS:                            104.193.88.123
IPV4 DESTINATION ADDRESS:                       192.168.20.200
TRNS SOURCE PORT:                               80
TRNS DESTINATION PORT:                          32964
IP VPN ID:                                      1000
IP PROTOCOL:                                    6
interface input:                                Tu2000000001
interface output:                               Gi3
counter bytes long:                             458
counter packets long:                           4
timestamp abs first:                            07:53:16.191
timestamp abs last:                             07:53:16.244
ulogging fw zp id:                              1
ulogging fw zone id array:                      1 2
ulogging fw class id:                           54049
ulogging fw policy id:                          29456
ulogging fw proto id:                           1
ulogging fw action:                             0
ulogging fw drop reason id:                     61
ulogging fw end flow reason:                    1
ulogging fw source ipv4 address translated:     10.1.1.1
ulogging fw destination ipv4 address translated: 20.1.1.1
ulogging fw source port translated:             0
ulogging fw destination port translated:        0
```

show flow record

To display FNF records, use the **show flow record** command in privileged EXEC mode.

show flow record

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	This command is supported in Cisco SD-WAN.

The following is sample output from the **show flow record** command that displays FNF records for cflowd events:

```
Router# show flow record
```

IPv4 flow record:

```
flow record sdwan_flow_record-1666223692122679:
  Description:        flow and application visibility records
  No. of users:       1
  Total field space:  102 bytes
  Fields:
    match ipv4 protocol
    match ipv4 source address
    match ipv4 destination address
    match transport source-port
    match transport destination-port
    match routing vrf service
    collect ipv4 dscp
    collect transport tcp flags
    collect interface input
    collect interface output
    collect counter bytes long
    collect counter packets long
    collect timestamp absolute first
    collect timestamp absolute last
    collect application name
    collect flow end-reason
    collect connection initiator
    collect overlay session id input
    collect overlay session id output
    collect connection id long
    collect drop cause id
    collect counter bytes sdwan dropped long
    collect sdwan sla-not-met
    collect sdwan preferred-color-not-met
    collect sdwan qos-queue-id
collect counter packets sdwan dropped long
```

IPv6 flow format:

```
flow record sdwan_flow_record_ipv6-1667963213662363:
  Description:        flow and application visibility records
  No. of users:       1
  Total field space:  125 bytes
```

```
Fields:
  match ipv6 protocol
  match ipv6 source address
  match ipv6 destination address
  match transport source-port
  match transport destination-port
  match routing vrf service
  collect ipv6 dscp
  collect transport tcp flags
  collect interface input
  collect interface output
  collect counter bytes long
  collect counter packets long
  collect timestamp absolute first
  collect timestamp absolute last
  collect application name
  collect flow end-reason
  collect connection initiator
  collect overlay session id input
  collect overlay session id output
  collect connection id long
  collect drop cause id
  collect counter bytes sdwan dropped long
  collect sdwan sla-not-met
  collect sdwan preferred-color-not-met
  collect sdwan qos-queue-id
  collect counter packets sdwan dropped long
```

show full-configuration probe-path load-balance-dia

To view the configured parameters for Cloud onRamp for SaaS load balancing, use the **show full-configuration probe-path load-balance-dia** command in configuration (config) mode.

show full-configuration probe-path load-balance-dia

Command Default

None

Command Modes

configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	This command was introduced.

Example

```
Device(config)#show full-configuration probe-path load-balance-dia
probe-path load-balance-dia latency-variance 50
probe-path load-balance-dia loss-variance 30
probe-path load-balance-dia source-ip-hash false
```

show geo file-contents info

To show the geodatabase file contents copied on the device from the Cisco.com download, use the **show geo file-contents info** command in privileged EXEC mode.

show geo file-contents info [**bootflash:** | **crashinfo:** | **flash:** | **webui:**]

Syntax Description

info	View the geolocation database file within the following folders: • bootflash • crashinfo • flash • webui

Command Default No geolocation database file information is displayed.

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines File content is displayed for the nondefault database only.

Examples

The following is example output from the **show geo file-contents info** command:

```
Device# show geo file-contents info bootflash:geo_ipv4_db
File version      : 2134.ajkdbnakjsdn
Number of entries : 415278
```

show geo status

To show the status of the geolocation database, use the **show geo status** command in privileged EXEC mode.

show geo status

Syntax Description This command has no arguments or keywords.

Command Default No geolocation database status information is displayed.

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Use the **show geo status** command to determine if the geolocation database is enabled or not.

Examples

The following are example outputs from the **show geo status** command:

```
Device# show geo status
Geo-Location Database is enabled
File in use       : Device default
```

```
Device# show geo status
Geo-Location Database has not been enabled.
```

show interfaces

To display statistics for all interfaces configured on the router, use the **show interfaces** command in privileged EXEC mode.

show interfaces [*type/number*] [**accounting** | **capabilities** | **counters** | **crb** | **dampening** | **debounce** | **description** | **etherchannel** | **flowcontrol** | **history** | **irb** | **mac-accounting** | **mpls-exp** | **mtu** | **precedence** | **private-vlan mapping** | **pruning** | **rate-limit** | **stats** | **status** | **summary** | **switch-port** | **transceiver** | **trunk**]

Syntax Description

None	Displays information for all interfaces.
type	(Optional) Interface type. Allowed values for type can be ACR, ATM-ACR, Analysis-Module, AppNav-Compress, AppNav-UnCompress, Async, Auto-Template, BD-VIF, BDI, BVI, Bluetooth, CDMA-Ix, CEM, CEM-ACR, CEM-PG, CTunnel, Container, Dialer, EsconPhy, Ethernet-Internal, Fcpa, Filter, Filtergroup, GMPLS, GigabitEthernet, IMA-ACR, LISP, LongReachEthernet, Loopback, Lspvif, MFR, Multilink, NVI, Null, Overlay, PROTECTION_GROUP, Port-channel, Portgroup, Pos-channel, SBC, SDH_ACR, SERIAL-ACR, SONET_ACR, SSLVPN-VIF, SYSCLOCK, Serial-PG, Service-Engine, TLS-VIF, Tunnel, Tunnel-tp, VPN, Vif, Vir-cem-ACR, Virtual-PPP, Virtual-Template, Virtual-TokenRing, Virtual-cem, VirtualPortGroup, Vlan, multiservice, nve, pseudowire, ucse, vasileft, vasiright, vmi, voaBypassIn, voaBypassOut, voaFilterIn, voaFilterOut, voaIn, voaOut.
number	(Optional) Port number on the selected interface.
accounting	(Optional) Displays the number of packets of each protocol type that have been sent through the interface.
capabilities	(Optional) Displays the interface capabilities for a module, an interface, or all interfaces.
counters	(Optional) Displays the current status of the protocol counters enabled.

crb	(Optional) Displays interface routing or bridging information.
dampening	(Optional) Displays interface dampening information.
debounce	(Optional) Displays the status and configuration for the debounce timer.
description	(Optional) Displays the interface description.
etherchannel	(Optional) Displays interface Ether Channel information.
flowcontrol	(Optional) Displays flow-control information.
history	(Optional) Displays histograms of interface utilization.
irb	(Optional) Displays interface routing or bridging information.
mac-accounting	(Optional) Displays interface MAC accounting information.
mpls-exp	(Optional) Displays interface Multiprotocol Label Switching (MPLS) experimental accounting information.
mtu	(Optional) Displays MTU information.
precedence	(Optional) Displays interface precedence accounting information.
private-vlan mapping	(Optional) Displays information about the private virtual local area network (PVLAN) mapping for VLAN SVIs.
pruning	(Optional) Displays the interface trunk VTP pruning information.
rate-limit	(Optional) Displays interface rate-limit information.
stats	(Optional) Displays interface packets and octets, in and out, by using switching path.
status	(Optional) Displays the interface status or a list of interfaces in an error-disabled state on local area network (LAN) ports only.
summary	(Optional) Displays interface summary.
switchport	(Optional) Displays the administrative and operational status of a switching (nonrouting) port.
transceiver	(Optional) Displays information about the optical transceivers that have digital optical monitoring (DOM) enabled.
trunk	(Optional) Displays the interface-trunk information.

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE show interfaces command.

Example

The following example shows how to display interface information on all interfaces.

```
Device# show interfaces
GigabitEthernet0/0/0 is up, line protocol is up
  Hardware is ISR4331-3x1GE, address is 084f.f99b.267c (bia 084f.f99b.267c)
  Description: INET
  Internet address is 10.3.6.2/24
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  Full Duplex, 1000Mbps, link type is auto, media type is RJ45
  output flow-control is off, input flow-control is off
  ARP type: ARPA, ARP Timeout 00:20:00
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 2000 bits/sec, 2 packets/sec
  5 minute output rate 1000 bits/sec, 1 packets/sec
     235182 packets input, 23708237 bytes, 0 no buffer
     Received 1 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 170048 multicast, 0 pause input
     71585 packets output, 12131971 bytes, 0 underruns
     Output 6 broadcasts (0 IP multicasts)
     0 output errors, 0 collisions, 1 interface resets
     1 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
GigabitEthernet0/0/1 is up, line protocol is up
  Hardware is ISR4331-3x1GE, address is 084f.f99b.267d (bia 084f.f99b.267d)
  Description: Service
  Internet address is 10.3.13.2/24
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  Full Duplex, 1000Mbps, link type is auto, media type is RJ45
  output flow-control is off, input flow-control is off
  ARP type: ARPA, ARP Timeout 00:20:00
  Last input 00:00:00, output 00:00:14, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     144332 packets input, 13390830 bytes, 0 no buffer
```

```
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 144332 multicast, 0 pause input
     13613 packets output, 5135370 bytes, 0 underruns
     Output 1 broadcasts (0 IP multicasts)
     0 output errors, 0 collisions, 1 interface resets
     1 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
<output truncated>
```

The following example shows how to display interface information on Loopback 65528.

```
Device# show interfaces Loopback 65528
Loopback65528 is up, line protocol is up
  Hardware is Loopback
  Internet address is 192.168.1.1/32
  MTU 1514 bytes, BW 8000000 Kbit/sec, DLY 5000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation LOOPBACK, loopback not set
  Keepalive set (10 sec)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     Output 0 broadcasts (0 IP multicasts)
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
```

The following example shows how to display interface descriptions.

```
Device# show interfaces description
Interface                      Status         Protocol Description
Gi0/0/0                        up             up       INET
Gi0/0/1                        up             up       Service
Gi0/0/2                        down           down
Gi0                            admin down     down
Sdwan-intf                     up             up
Lo65528                        up             up
NV0                            up             up
Tu0                            up             up
```

The following example shows how to display the number of packets of each protocol type that have been sent through the interface.

```
Device# show interface accounting
GigabitEthernet0/0/0 INET
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
                   Other     169551   14869854      39712    6645521
                      IP      66732    8948821      32339    5548047
          Spanning Tree     259684   13763252          0          0
                     ARP      26188    1571280      26193    1571580
                     CDP       4818    2009106       4815    2123285
                    LLDP       8702    3498204       8704    2950656
```

```
GigabitEthernet0/0/1 Service
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
                   Other     143370   13301850      13521    5100639
           Spanning Tree     259682   13763146          0          0
                     ARP          0          0          1         60
                     CDP       4826    2012442       4817    2124153
                    LLDP       8702    3498204       8704    2976768
GigabitEthernet0/0/2
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
No traffic sent or received on this interface.
Interface GigabitEthernet0 is disabled
SDWAN System Intf IDB
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
No traffic sent or received on this interface.
Loopback65528
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
No traffic sent or received on this interface.
NVI0
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
No traffic sent or received on this interface.
Tunnel0
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
No traffic sent or received on this interface.
```

The following example shows how to display interfaces summary.

```
Device# show interface summary

 *: interface is up
 IHQ: pkts in input hold queue     IQD: pkts dropped from input queue
 OHQ: pkts in output hold queue    OQD: pkts dropped from output queue
 RXBS: rx rate (bits/sec)          RXPS: rx rate (pkts/sec)
 TXBS: tx rate (bits/sec)          TXPS: tx rate (pkts/sec)
 TRTL: throttle count

  Interface                   IHQ        IQD       OHQ       OQD      RXBS      RXPS
TXBS      TXPS      TRTL
------------------------------------------------------------------------------------------------------------
* GigabitEthernet0/0/0          0          0         0         0      4000         6
3000         3         0
* GigabitEthernet0/0/1          0          0         0         0         0         0
  0         0         0
  GigabitEthernet0/0/2          0          0         0         0         0         0
  0         0         0
  GigabitEthernet0              0          0         0         0         0         0
  0         0         0
* Sdwan-system-intf             0          0         0         0         0         0
  0         0         0
* Loopback65528                 0          0         0         0         0         0
  0         0         0
* NVI0                          0          0         0         0         0         0
  0         0         0
* Tunnel0                       0          0         0         4         0         0
  0         0         0
```

show interface port-channel

To display the general status of the port channel interface, use the **show interface port-channel** command in privileged EXEC mode.

show interface port-channel

Command Default

None

Command Modes

Privileged EXEC (>)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	This command was introduced.

Examples

The following sample output displays the status of port channel 10.

```
Device# show interface port-channel 10
 Port-channel10 is up, line protocol is up

  Hardware is 10GEChannel, address is a8b4.5606.ddc9 (bia a8b4.5606.ddc9)

  MTU 1500 bytes, BW 20000000 Kbit/sec, DLY 10 usec,

     reliability 255/255, txload 1/255, rxload 1/255

  Encapsulation ARPA, loopback not set

  Keepalive set (10 sec)

  ARP type: ARPA, ARP Timeout 04:00:00

    No. of active members in this channel: 2

        Member 0 : TenGigabitEthernet0/1/0 , Full-duplex, 10000Mb/s

        Member 1 : TenGigabitEthernet0/1/1 , Full-duplex, 10000Mb/s

    No. of PF_JUMBO supported members in this channel : 2

  Last input never, output never, output hang never

  Last clearing of "show interface" counters 00:39:12

  Input queue: 0/750/0/0 (size/max/drops/flushes); Total output drops: 0

  Queueing strategy: fifo

  Output queue: 0/80 (size/max)

  5 minute input rate 0 bits/sec, 0 packets/sec

  5 minute output rate 0 bits/sec, 0 packets/sec

     0 packets input, 0 bytes, 0 no buffer

     Received 0 broadcasts (0 IP multicasts)

     0 runts, 0 giants, 0 throttles

     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored

     0 watchdog, 0 multicast, 0 pause input
```

```
     0 packets output, 0 bytes, 0 underruns
     Output 0 broadcasts (0 IP multicasts)

     0 output errors, 0 collisions, 0 interface resets

     0 unknown protocol drops

     0 babbles, 0 late collision, 0 deferred

     0 lost carrier, 0 no carrier, 0 pause output

     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
```

show interface port-channel etherchannel

To display information about a specific port channel interface, use the **show interface port-channel etherchannel** command in privileged EXEC mode.

show interface port-channel *channel-number* **etherchannel**

Command Default

None

Command Modes

Privileged EXEC (>)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	This command was introduced.

Examples

The following sample output displays the information about port channel 10.

```
Device# show interface port-channel 10 etherchannel
Flags:  D - down        P/bndl - bundled in port-channel
        I - stand-alone s/susp - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


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

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1       Po1(RU)         LACP     Te0/3/0(bndl) Te0/3/1(hot-sby)

RU - L3 port-channel UP State
SU - L2 port-channel UP state
P/bndl -  Bundled
```

```
S/susp  - Suspended
```

show inventory

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

show inventory [*entity* | **fru** *entity* | **oid** *entity* | **raw** *entity*]

Syntax Description

entity	(Optional) Name of a Cisco entity (for example, chassis, backplane, module, or slot). A quoted string may be used to display a specific UDI information; for example “module 0” displays UDI information for slot 0 of an entity named module.
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).
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.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

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 sub-entities 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.

Example

The following example shows how to display the inventory in the device.

```
Device# show inventory

++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
INFO: Please use "show license UDI" to get serial number for licensing.
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++

NAME: "Chassis", DESCR: "Cisco ISR4331 Chassis"
PID: ISR4331/K9         , VID: V05  , SN: SAMPLESN123
NAME: "Power Supply Module 0", DESCR: "250W AC Power Supply for Cisco ISR 4330"
PID: PWR-4330-AC        , VID: V03  , SN: SAMPLESN123
NAME: "Fan Tray", DESCR: "Cisco ISR4330 Fan Assembly"
PID: ACS-4330-FANASSY   , VID:      , SN:
NAME: "module 0", DESCR: "Cisco ISR4331 Built-In NIM controller"
PID: ISR4331/K9         , VID:      , SN:
NAME: "NIM subslot 0/0", DESCR: "Front Panel 3 ports Gigabitethernet Module"
PID: ISR4331-3x1GE      , VID: V01  , SN:
NAME: "module 1", DESCR: "Cisco ISR4331 Built-In SM controller"
PID: ISR4331/K9         , VID:      , SN:
NAME: "module R0", DESCR: "Cisco ISR4331 Route Processor"
PID: ISR4331/K9         , VID: V05  , SN: SAMPLESN123
NAME: "module F0", DESCR: "Cisco ISR4331 Forwarding Processor"
PID: ISR4331/K9         , VID:      , SN:
```

The following example shows how to display the inventory in the device with an entity argument value.

```
Device# show inventory "module 0"

++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
INFO: Please use "show license UDI" to get serial number for licensing.
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++

NAME: "module 0", DESCR: "Cisco ISR4331 Built-In NIM controller"
PID: ISR4331/K9         , VID:      , SN:
NAME: "NIM subslot 0/0", DESCR: "Front Panel 3 ports Gigabitethernet Module"
PID: ISR4331-3x1GE      , VID: V01  , SN:
```

The following example shows how to display the inventory in the device with oid argument value.

```
Device# show inventory oid

++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
INFO: Please use "show license UDI" to get serial number for licensing.
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
NAME: "Chassis", DESCR: "Cisco ISR4331 Chassis"
PID: ISR4331/K9         , VID: V05  , SN: SAMPLESN123
OID: 1.3.6.1.4.1.9.12.3.1.3.1544
NAME: "Power Supply Module 0", DESCR: "250W AC Power Supply for Cisco ISR 4330"
PID: PWR-4330-AC        , VID: V03  , SN: SAMPLESN123
OID: 1.3.6.1.4.1.9.12.3.1.6.442
NAME: "Fan Tray", DESCR: "Cisco ISR4330 Fan Assembly"
PID: ACS-4330-FANASSY   , VID:      , SN:
OID: 1.3.6.1.4.1.9.12.3.1.7.244
NAME: "module 0", DESCR: "Cisco ISR4331 Built-In NIM controller"
PID: ISR4331/K9         , VID:      , SN:
OID: 1.3.6.1.4.1.9.12.3.1.9.104.8
```

```
NAME: "NIM subslot 0/0", DESCR: "Front Panel 3 ports Gigabitethernet Module"
PID: ISR4331-3x1GE     , VID: V01  , SN:
OID: 1.3.6.1.4.1.9.12.3.1.9.104.5
NAME: "module 1", DESCR: "Cisco ISR4331 Built-In SM controller"
PID: ISR4331/K9        , VID:      , SN:
OID: 1.3.6.1.4.1.9.12.3.1.9.104.9
NAME: "module R0", DESCR: "Cisco ISR4331 Route Processor"
PID: ISR4331/K9        , VID: V05  , SN: SAMPLESN123
OID: 1.3.6.1.4.1.9.12.3.1.9.104.6
NAME: "module F0", DESCR: "Cisco ISR4331 Forwarding Processor"
PID: ISR4331/K9        , VID:      , SN:
OID: 1.3.6.1.4.1.9.12.3.1.9.104.7
```

Table 77: Related Commands

Commands	Description
show license udi	Shows license UDI information.

show idmgr status

To display the Identity Manager status for its connections to SD-WAN Manager, use the **show idmgr status** command in privileged EXEC mode.

show idmgr status

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This command was introduced.
SD-WAN Manager 20.18.2	This command was updated from **show idmgr pxgrid-status** to **show idmgr status**

Examples

The following sample output displays the Identity Manager status for pxGrid connections.

```
Device# show idmgr status
----------------------------------------
Identity Manager Status
----------------------------------------
Manager address                192.168.1.1
Websocket status               ws-connected
WS base path                   vmanage/iseproxy
Last notification sent         Manager websocket connection has been established
```

Related Commands

Command	Description
show idmgr omp ip-user-bindings	Displays ip-user session bindings sent to OMP.

Command	Description
show idmgr omp user-usergroup-bindings	Displays user-usergroup bindings sent to OMP.
show idmgr user-sessions	Displays users essions learnt from Cisco ISE.

show idmgr omp ip-user-bindings

To display the ip-user session bindings sent to OMP, use the **show idmgr omp ip-user-bindings** command in privileged EXEC mode.

show idmgr omp ip-user-bindings

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This command was introduced.

Examples

The following sample output displays the ip-user session bindings sent to OMP.

```
Device# show idmgr omp ip-user-bindings
IP                                                OMP UPDATE
ADDRESS   USERNAME                                STATE
-----------------------------------------------------------
72.1.1.7  TestUser0@SDWAN-IDENTITY.CISCO.COM  omp-updated
```

Related Commands

Command	Description
show idmgr pxgrid-status	Displays Identity Manager status for pxGrid connections.
show idmgr omp user-usergroup-bindings	Displays user-usergroup bindings sent to OMP.
show idmgr user-sessions	Displays users sessions learned from Cisco ISE.

show idmgr omp user-usergroup-bindings

To display the user-usergroup bindings sent to OMP, use the **show idmgr omp user-usergroup-bindings** command in privileged EXEC mode.

show idmgr omp user-usergroup-bindings

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This command was introduced.

Examples

The following sample output displays the user-usergroup bindings sent to OMP.

```
Device# show idmgr omp user-usergroup-bindings
idmgr omp user-usergroup-bindings TestUser0@SDWAN-IDENTITY.CISCO.COM
 user-groups      "Unknown sdwan-identity.cisco.com/S-1-5-32-545
S-1-5-21-787885371-2815506856-1818290038-513 SDWAN-IDENTITY.CISCO.COM/Builtin/Users
SDWAN-IDENTITY.CISCO.COM/Users/Domain Users "
 omp-update-state omp-updated
idmgr omp user-usergroup-bindings TestUser1@SDWAN-IDENTITY.CISCO.COM
 user-groups      "Unknown sdwan-identity.cisco.com/S-1-5-32-545
S-1-5-21-787885371-2815506856-1818290038-513 SDWAN-IDENTITY.CISCO.COM/Builtin/Users
SDWAN-IDENTITY.CISCO.COM/Users/Domain Users "
 omp-update-state omp-updated
idmgr omp user-usergroup-bindings adsclient
 user-groups      "User Identity Groups:Employee User Identity Groups:TestUserGroup-1 null
 null "
 omp-update-state omp-updated
```

Related Commands

Command	Description
show idmgr pxgrid-status	Displays Identity Manager status for pxGrid connections.
show idmgr omp ip-user-bindings	Displays the ip-user session bindings sent to OMP.
show idmgr user-sessions	Displays users sessions learned from Cisco ISE.

show idmgr user-sessions

To display the user sessions learned from Cisco ISE, use the **show idmgr user-sessions** command in privileged EXEC mode.

show idmgr user-sessions

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This command was introduced.

Examples

The following sample output displays the user sessions learnt from ISE.

```
Device# show idmgr user-sessions

USERNAME                                ADDRESS   TIMESTAMP                       STATE

-------------------------------------------------------------------------------------------
TestUser0@SDWAN-IDENTITY.CISCO.COM  72.1.1.7  2022-02-18T13:00:54.372-05:00  Authenticated
```

Related Commands

Command	Description
show idmgr pxgrid-status	Displays Identity Manager status for pxGrid connections.
show idmgr omp ip-user-bindings	Displays the ip-user session bindings sent to OMP.
show idmgr omp user-usergroup-bindings	Displays the user-usergroup bindings sent to OMP.

show ip bgp ipv4

To display entries in the IP version 4 (IPv4) BGP unicast database-related information **show ip bgp ipv4 unicast** command in privileged EXEC mode.

show [**ip**] **bgp ipv4 unicast** [*command*]

Syntax Description

prefix-list	(Optional) Displays entries for the specified prefix.
commad	(Optional) Any multiprotocol BGP command unicast commands supported by the **show ip bgp ipv4 unicast** command.

Command Modes

Privileged EXEC (#)

Examples

The following is sample output from the **show ip bgp ipv4 unicast** command:

```
Device# show ip bgp ipv4 unicast

 BGP table version is 4, local router ID is 10.0.40.1
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
*> 10.10.10.0/24   172.16.10.1              0             0  300 i
*> 10.10.20.0/24   172.16.10.1              0             0  300 i
*  10.20.10.0/24   172.16.10.1              0             0  300 i
```

The following is sample output from the **show ip bgp ipv4 multicast** command:

```
Device# show ip bgp ipv4 multicast

 BGP table version is 4, local router ID is 10.0.40.1
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
*> 10.10.10.0/24   172.16.10.1              0             0  300 i
```

```
*> 10.10.20.0/24    172.16.10.1              0             0  300 i
*  10.20.10.0/24    172.16.10.1              0             0  300 i
```

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

Table 78: show ip bgp ipv4 unicast 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.
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: • s—The table entry is suppressed. • d—The table entry is damped. • 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 Border Gateway Protocol (IBGP) session.
Origin codes	Origin of the entry. The origin code is displayed at the end of each line in the table. It can be one of the following values: • 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.
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.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

The following is sample output from the **show ip bgp ipv4 unicast** *prefix* command. The output indicates the imported path information from a VRF named vpn1.

```
Device# show ip bgp ipv4 unicast 192.168.1.0

BGP routing table entry for 10.1.1.0/24, version 2
Paths: (1 available, best #1, table default)
  Not advertised to any peer
  Refresh Epoch 1
  65002, imported path from 1:1:192.168.1.0/24 (vpn1)
    10.4.4.4 (metric 11) from 10.4.4.4 (10.4.4.4)
      Origin IGP, metric 0, localpref 100, valid, internal, best
      Extended Community: RT:1:1
      mpls labels in/out nolabel/16
```

The following is sample output from the **show ip bgp ipv4 unicast** *prefix* **best-path-reason** command. (The **best-path-reason** keyword was added in Cisco IOS XE Gibralter 16.10.1.)

Prior to running the command, the best path has already been determined. Each path is compared to the best path. The line that starts with **Best Path Evaluation:** shows the reason why this path is not the preferred path, compared to the best path. Possible reasons include: **Lower local preference**, and **Longer cluster length**. The best path shows the reason: **Overall best path**.

```
Router# show ip bgp 172.16.70.96 bestpath-reason
BGP routing table entry for 172.16.0.0/16, version 59086010
Paths: (3 available, best #2, table default)
Multipath: eBGP  Advertised to update-groups:   1  2  3  5  6  7  8  9
  3491 5486, (received & used)
    203.0.113.126 (metric 12989) from 198.51.100.13 (198.51.100.13)
      Origin EGP, metric 0, localpref 300, valid, internal
      Community: 3549:4713 3549:31276
      Originator: 198.51.100.84, Cluster list: 0.0.0.91, 0.0.0.121
      Best Path Evaluation: Lower local preference
  3491 5486, (received & used)
    203.0.113.126 (metric 12989) from 198.51.100.210  (198.51.100.210 )
      Origin EGP, metric 0, localpref 300, valid, internal, best
      Community: 3549:4713 3549:31276
      Originator: 198.51.100.84, Cluster list: 0.0.0.91, 0.0.0.121
      Best Path Evaluation: Overall best path
    203.0.113.126 (metric 12989) from 198.51.100.210  (198.51.100.210 )
      Origin EGP, metric 0, localpref 300, valid, internal
      Community: 3549:4713 3549:31276
      Originator: 198.51.100.84, Cluster list: 0.0.0.91, 0.0.0.121
      Best Path Evaluation: Longer cluster length
```

show ip bgp vpnv4

To display VPN Version 4 (VPNv4) address information from the Border Gateway Protocol (BGP) table, use the **show ip bgp vpnv4** command in user EXEC or privileged EXEC mode.

show ip bgp vpnv4 [*command*]

Syntax Description

command	(Optional) Any BGP command supported by the **show ip bgp vpnv4** command .

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
16.9	This command was introduced.

Usage Guidelines

Use this command to display VPNv4 information from the BGP database. The **show ip bgp vpnv4 all** command displays all available VPNv4 information. The **show ip bgp vpnv4 all summary** command displays BGP neighbor status. The **show ip bgp vpnv4 all labels** command displays label information.

Examples

The following example shows all available VPNv4 information in a BGP routing table:

```
Device# show ip bgp vpnv4 all

BGP table version is 18, local router ID is 10.14.14.14
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
Route Distinguisher: 1:101 (default for vrf vpn1)
*>i10.6.6.6/32       10.0.0.21               11    100      0 ?
*> 10.7.7.7/32       10.150.0.2              11         32768 ?
*>i10.69.0.0/30      10.0.0.21                0    100      0 ?
*> 10.150.0.0/24     0.0.0.0                  0         32768 ?
```

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

Table 79: show ip bgp vpnv4 all Field Descriptions

Field	Description
Network	Displays the network address from the BGP table.
Next Hop	Displays the address of the BGP next hop.
Metric	Displays the BGP metric.
LocPrf	Displays the local preference.
Weight	Displays the BGP weight.
Path	Displays the BGP path per route.

The following example shows how to display a table of labels for NLRI prefixes that have a route distinguisher value of 100:1.

```
Device# show ip bgp vpnv4 rd 100:1 labels

Network            Next Hop       In label/Out label
Route Distinguisher: 100:1 (vrf1)
   10.0.0.0         10.20.0.60      34/nolabel
   10.0.0.0         10.20.0.60      35/nolabel
   10.0.0.0         10.20.0.60      26/nolabel
                    10.20.0.60      26/nolabel
   10.0.0.0         10.15.0.15      nolabel/26
```

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

Table 80: show ip bgp vpnv4 rd labels Field Descriptions

Field	Description
Network	Displays the network address from the BGP table.
Next Hop	Specifies the BGP next hop address.
In label	Displays the label (if any) assigned by this router.
Out label	Displays the label assigned by the BGP next-hop router.

The following example shows VPNv4 routing entries for the VRF named vpn1:

```
Device# show ip bgp vpnv4 vrf vpn1

BGP table version is 18, local router ID is 10.14.14.14
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
Route Distinguisher: 100:1 (default for vrf test1)
*> 10.1.1.1/32      192.168.1.1              0             0 100 i
*bi                 10.4.4.4                 0    100      0 100 i
*> 10.2.2.2/32      192.168.1.1                            0 100 i
*bi                 10.4.4.4                 0    100      0 100 i
*> 172.16.1.0/24    192.168.1.1              0             0 100 i
* i                 10.4.4.4                 0    100      0 100 i
r> 192.168.1.0      192.168.1.1              0             0 100 i
rbi                 10.4.4.4                 0    100      0 100 i
*> 192.168.3.0      192.168.1.1                            0 100 i
*bi                 10.4.4.4                 0    100      0 100 i
```

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

Table 81: show ip bgp vpnv4 vrf Field Descriptions

Field	Description
Network	Displays the network address from the BGP table.
Next Hop	Displays the address of the BGP next hop.
Metric	Displays the BGP metric.
LocPrf	Displays the local preference.
Weight	Displays the BGP weight.
Path	Displays the BGP path per route.

The following example shows attributes for network 192.168.9.0 that include multipaths, best path, and a recursive-via-host flag:

```
Device# show ip bgp vpnv4 vrf vpn1 192.168.9.0 255.255.255.0

BGP routing table entry for 100:1:192.168.9.0/24, version 44
Paths: (2 available, best #2, table test1)
  Additional-path
  Advertised to update-groups:
     2
  100, imported path from 400:1:192.168.9.0/24
    10.8.8.8 (metric 20) from 10.5.5.5 (10.5.5.5)
      Origin IGP, metric 0, localpref 100, valid, internal, backup/repair
      Extended Community: RT:100:1 RT:200:1 RT:300:1 RT:400:1
      Originator: 10.8.8.8, Cluster list: 10.5.5.5 , recursive-via-host
      mpls labels in/out nolabel/17
  100, imported path from 300:1:192.168.9.0/24
    10.7.7.7 (metric 20) from 10.5.5.5 (10.5.5.5)
      Origin IGP, metric 0, localpref 100, valid, internal, best
      Extended Community: RT:100:1 RT:200:1 RT:300:1 RT:400:1
      Originator: 10.7.7.7, Cluster list: 10.5.5.5 , recursive-via-host
      mpls labels in/out nolabel/17
```

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

Table 82: show ip bgp vpnv4 all network-address Field Descriptions

Field	Description
BGP routing table entry for ... version	Internal version number of the table. This number is incremented whenever the table changes.
Paths	Number of autonomous system paths to the specified network. If multiple paths exist, one of the multipaths is designated the best path.
Multipath	Indicates the maximum paths configured (iBGP or eBGP).
Advertised to non peer-group peers	IP address of the BGP peers to which the specified route is advertised.
10.22.7.8 (metric 11) from 10.11.3.4 (10.0.0.8)	Indicates the next hop address and the address of the gateway that sent the update.
Origin	Indicates the origin of the entry. It can be one of the following values: • IGP—Entry originated from Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. • incomplete—Entry originated from other than an IGP or Exterior Gateway Protocol (EGP) and was advertised with the **redistribute** router configuration command. • EGP—Entry originated from an EGP.
metric	If shown, the value of the interautonomous system metric.
localpref	Local preference value as set with the **set local-preference route-map** configuration command. The default value is 100.
valid	Indicates that the route is usable and has a valid set of attributes.

Field	Description
internal/external	The field is internal if the path is learned via iBGP. The field is external if the path is learned via eBGP.
multipath	One of multiple paths to the specified network.
best	If multiple paths exist, one of the multipaths is designated the best path and this path is advertised to neighbors.
Extended Community	Route Target value associated with the specified route.
Originator	The router ID of the router from which the route originated when route reflector is used.
Cluster list	The router ID of all the route reflectors that the specified route has passed through.

The following example shows routes that BGP could not install in the VRF table:

```
Device# show ip bgp vpnv4 vrf xyz rib-failure

Network            Next Hop                      RIB-failure   RIB-NH Matches
Route Distinguisher: 2:2 (default for vrf bar)
10.1.1.2/32        10.100.100.100      Higher admin distance              No
10.111.111.112/32  10.9.9.9            Higher admin distance             Yes
```

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

Table 83: show ip bgp vpnv4 vrf rib-failure Field Descriptions

Field	Description
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.
RIB-failure	Cause of the Routing Information Base (RIB) failure. Higher admin distance means that a route with a better (lower) administrative distance, such as a static route, already exists in the IP routing table.
RIB-NH Matches	Route status that applies only when Higher admin distance appears in the RIB-failure column and the **bgp suppress-inactive** command is configured for the address family being used. There are three choices: • Yes—Means that the route in the RIB has the same next hop as the BGP route or that the next hop recurses down to the same adjacency as the BGP next hop. • No—Means that the next hop in the RIB recurses down differently from the next hop of the BGP route. • n/a—Means that the **bgp suppress-inactive** command is not configured for the address family being used.

NSF/SSO: MPLS VPN

The following example shows the information displayed on the active and standby Route Processors when they are configured for NSF/SSO: MPLS VPN.

Active Route Processor

```
Device# show ip bgp vpnv4 all labels

Network          Next Hop   In label/Out label
Route Distinguisher: 100:1 (vpn1)
10.12.12.12/32  0.0.0.0    16/aggregate(vpn1)
10.0.0.0/8      0.0.0.0    17/aggregate(vpn1)
Route Distinguisher: 609:1 (vpn0)
10.13.13.13/32  0.0.0.0    18/aggregate(vpn0)

Router# show ip bgp vpnv4 vrf vpn1 labels

Network          Next Hop   In label/Out label
Route Distinguisher: 100:1 (vpn1)
10.12.12.12/32   0.0.0.0    16/aggregate(vpn1)
10.0.0.0/8       0.0.0.0    17/aggregate(vpn1)
```

Standby Route Processor

```
Device# show ip bgp vpnv4 all labels

Network       Masklen   In label
Route Distinguisher: 100:1
10.12.12.12   /32       16
10.0.0.0      /8        17
Route Distinguisher: 609:1
10.13.13.13   /32       18

Router# show ip bgp vpnv4 vrf vpn1 labels

Network        Masklen   In label
Route Distinguisher: 100:1
10.12.12.12    /32       16
10.0.0.0       /8        17
```

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

Table 84: show ip bgp vpnv4 labels Field Descriptions

Field	Description
Network	The network address from the BGP table.
Next Hop	The BGP next-hop address.
In label	The label (if any) assigned by this router.
Out label	The label assigned by the BGP next-hop router.
Masklen	The mask length of the network address.

The following example displays output, including the explicit-null label, from the **show ip bgp vpnv4 all labels** command on a CSC-PE router:

```
Device# show ip bgp vpnv4 all labels

   Network          Next Hop      In label/Out label
Route Distinguisher: 100:1 (v1)
   10.0.0.0/24      10.0.0.0        19/aggregate(v1)
   10.0.0.1/32      10.0.0.0        20/nolabel
   10.1.1.1/32      10.0.0.0        21/aggregate(v1)
   10.10.10.10/32   10.0.0.1        25/exp-null

   10.168.100.100/32
                    10.0.0.1        23/exp-null
   10.168.101.101/32
                    10.0.0.1        22/exp-null
```

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

Table 85: show ip bgp vpnv4 all labels Field Descriptions

Field	Description
Network	Displays the network address from the BGP table.
Next Hop	Displays the address of the BGP next hop.
In label	Displays the label (if any) assigned by this router.
Out label	Displays the label assigned by the BGP next-hop router.
Route Distinguisher	Displays an 8-byte value added to an IPv4 prefix to create a VPN IPv4 prefix.

The following example displays separate router IDs for each VRF in the output. The router ID is shown next to the VRF name.

```
Device# show ip bgp vpnv4 all

BGP table version is 5, local router ID is 172.17.1.99
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
Route Distinguisher: 1:1 (default for vrf vrf_trans) VRF Router ID 10.99.1.2
*> 192.168.4.0      0.0.0.0                  0         32768 ?
Route Distinguisher: 42:1 (default for vrf vrf_user) VRF Router ID 10.99.1.1
*> 192.168.5.0      0.0.0.0                  0         32768 ?
```

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

Table 86: show ip bgp vpnv4 all (VRF Router ID) Field Descriptions

Field	Description
Route Distinguisher	Displays an 8-byte value added to an IPv4 prefix to create a VPN IPv4 prefix.
vrf	Name of the VRF.

Field	Description
VRF Router ID	Router ID for the VRF.

BGP Event-Based VPN Import

In the following example, the BGP Event-Based VPN Import feature is configured. When the **import path selection** command is configured, but the **strict** keyword is not included, then a safe import path selection policy is in effect. When a path is imported as the best available path (when the best path or multipaths are not eligible for import), the imported path includes the wording "imported safety path," as shown in the output.

```
Device# show ip bgp vpnv4 all 172.17.0.0

BGP routing table entry for 45000:1:172.17.0.0/16, version 10
Paths: (1 available, best #1, table vrf-A)
Flag: 0x820
   Not advertised to any peer
   2, imported safety path from 50000:2:172.17.0.0/16
     10.0.101.1 from 10.0.101.1 (10.0.101.1)
       Origin IGP, metric 200, localpref 100, valid, internal, best
       Extended Community: RT:45000:100
```

In the following example, BGP Event-Based VPN Import feature configuration information is shown. When the **import path selection** command is configured with the **all** keyword, any path that matches an RD of the specified VRF will be imported, even though the path does not match the Route Targets (RT) imported by the specified VRF. In this situation, the imported path is marked as "not-in-vrf" as shown in the output. Note that on the net for vrf-A, this path is not the best path because any paths that are not in the VRFs appear less attractive than paths in the VRF.

```
Device# show ip bgp vpnv4 all 172.17.0.0

BBGP routing table entry for 45000:1:172.17.0.0/16, version 11
Paths: (2 available, best #2, table vrf-A)
Flag: 0x820
   Not advertised to any peer
   2
     10.0.101.2 from 10.0.101.2 (10.0.101.2)
       Origin IGP, metric 100, localpref 100, valid, internal, not-in-vrf
       Extended Community: RT:45000:200
       mpls labels in/out nolabel/16
   2
     10.0.101.1 from 10.0.101.1 (10.0.101.1)
       Origin IGP, metric 50, localpref 100, valid, internal, best
       Extended Community: RT:45000:100
mpls labels in/out nolabel/16
```

In the following example, the unknown attributes and discarded attributes associated with the prefix are displayed.

```
Device# show ip bgp vpnv4 all 10.0.0.0/8

BGP routing table entry for 100:200:10.0.0.0/8, version 0
Paths: (1 available, no best path)
  Not advertised to any peer
  Refresh Epoch 1
  Local
```

```
    10.0.103.1 from 10.0.103.1 (10.0.103.1)
      Origin IGP, localpref 100, valid, internal
      Extended Community: RT:1:100
      Connector Attribute: count=1
       type 1 len 12 value 22:22:10.0.101.22
      mpls labels in/out nolabel/16
      unknown transitive attribute: flag E0 type 129 length 32
        value 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000
      unknown transitive attribute: flag E0 type 140 length 32
        value 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000
      unknown transitive attribute: flag E0 type 120 length 32
        value 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000
      discarded unknown attribute: flag C0 type 128 length 32
        value 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000
```

BGP—VPN Distinguisher Attribute

The following example is based on the BGP—VPN Distinguisher Attribute feature. The output displays an Extended Community attribute, which is the VPN distinguisher (VD) of 104:1.

```
Device# show ip bgp vpnv4 unicast all 1.4.1.0/24

BGP routing table entry for 104:1:1.4.1.0/24, version 28
Paths: (1 available, best #1, no table)
   Advertised to update-groups:
      1
   Refresh Epoch 1
   1001
     19.0.101.1 from 19.0.101.1 (19.0.101.1)
       Origin IGP, localpref 100, valid, external, best
       Extended Community: VD:104:1
       mpls labels in/out nolabel/16
       rx pathid: 0, tx pathid: 0x0
```

BGP—Support for iBGP Local-AS

The following example includes “allow-policy” in the output, indicating that the BGP—Support for iBGP Local-AS feature was configured for the specified neighbor by configuring the **neighbor allow-policy** command.

```
Device# show ip bgp vpnv4 all neighbors 192.168.3.3 policy

Neighbor: 192.168.3.3, Address-Family: VPNv4 Unicast
Locally configured policies:
 route-map pe33 out
 route-reflector-client
 allow-policy
 send-community both
```

show ip bgp vpnv4 vrf

To display VPN Version 4 (VPNv4) information for a VRF Routing/Forwarding instance from the Border Gateway Protocol (BGP) table, use the **show ip bgp vpnv4 vrf** command in privileged EXEC mode.

show ip bgp vpnv4 vrf *vrf-number*

Syntax Description

vrf-number	Specifies the vrf number to be displayed.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Use this command to display VPN Version 4 (VPNv4) Network information for a VRF Routing/Forwarding instance from the Border Gateway Protocol (BGP) table.

Example

The following example shows how to display the VPNv4 BGP routing table information from VRF.

```
Device# show ip bgp vpnv4 vrf 1
BGP table version is 18, local router ID is 10.14.14.14
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
Route Distinguisher: 100:1 (default for vrf test1)
*> 10.1.1.1/32 192.168.1.1 0 0 100 i
*bi 10.4.4.4 0 100 0 100 i
*> 10.2.2.2/32 192.168.1.1 0 100 i
*bi 10.4.4.4 0 100 0 100 i
*> 172.16.1.0/24 192.168.1.1 0 0 100 i
* i 10.4.4.4 0 100 0 100 i
r> 192.168.1.0 192.168.1.1 0 0 100 i
rbi 10.4.4.4 0 100 0 100 i
*> 192.168.3.0 192.168.1.1 0 100 i
*bi 10.4.4.4 0 100 0 100 i
```

Table 87: Related Commands

Commands	Description
show ip bgp vpnv4 all	Displays information about all VPN NLRIs.
show ip bgp vpnv4 rd	Displays information for a route distinguisher.

show ip dhcp binding

To display the current DHCP lease bindings, including assigned IP addresses, client identifiers, lease expiration times, and binding states, use the **show ip dhcp binding** command in privileged EXEC mode.

show ip dhcp binding

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This command is supported in Cisco Catalyst SD-WAN.

Usage Guidelines

The **show ip dhcp binding** command is essential for verifying the operational status of your DHCP server and for confirming DHCP lease synchronization in a high availability setup. When troubleshooting or verifying DHCP high availability, execute this command on both the active and standby Cisco IOS XE Catalyst SD-WAN devices. The output should display identical lease information on both devices, indicating successful state synchronization.

Examples

The following is a sample output from the **show ip dhcp binding** command showing active DHCP leases within VRF pool 1:

```
Device# show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address      Client-ID/   Lease expiration  Type       State      Interface
  Hardware address/
  User name

Bindings from VRF pool 1:
IP address      Client-ID/   Lease expiration  Type       State      Interface
  Hardware address/
  User name
10.20.93.203    0063.6973.636f.2d35.    Sep 04 2025 09:47 AM    Automatic  Active
FortyGigabitEthernet0/2/0
                3235.342e.3030.6661.
                2e38.6161.302d.4769.
                33
10.20.93.236    000c.2900.77a5          Sep 04 2025 09:46 AM    Automatic  Active
FortyGigabitEthernet0/2/0
10.20.93.237    000c.2900.77a6          Sep 04 2025 09:46 AM    Automatic  Active
FortyGigabitEthernet0/2/0
10.20.93.238    000c.2900.77a7          Sep 04 2025 09:46 AM    Automatic  Active
FortyGigabitEthernet0/2/0
10.20.93.239    000c.2900.77a8          Sep 04 2025 09:46 AM    Automatic  Active
FortyGigabitEthernet0/2/0
10.20.93.240    000c.2900.77a9          Sep 04 2025 09:46 AM    Automatic  Active
FortyGigabitEthernet0/2/0
10.20.93.241    000c.2900.77aa          Sep 04 2025 09:46 AM    Automatic  Active
FortyGigabitEthernet0/2/0
10.20.93.242    000c.2900.77ab          Sep 04 2025 09:46 AM    Automatic  Active
FortyGigabitEthernet0/2/0
```

show ip cef vrf

To display the Cisco Express Forwarding forwarding table associated with a Virtual Private Network (VPN) routing or forwarding instance (VRF), use the **show ip cef vrf** command in privileged EXEC mode.

show ip cef vrf *vrf-name ip-prefix* **internal**

Syntax Description

vrf-name	Specifies the name of the VRF from which routes are replicated.
ip-prefix	(Optional) IP prefix of entries to show, in dotted decimal format (A.B.C.D).
internal	Display internal data structures.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This command was introduced.

Usage Guidelines

Used with only the vrf-name argument, the **show ip cef vrf** command shows a shortened display of the Cisco Express Forwarding table.

Used with the **internal** keyword, the **show ip cef vrf** command shows internal data structures information for all Cisco Express Forwarding table entries.

Examples

The following is a sample output from the **show ip cef vrf** command that shows the replicated routes from VRF 1:

```
Device# show ip cef vrf 2 10.10.10.97 internal
10.10.10.97/32, epoch 0, RIB[S], refcnt 6, per-destination sharing
  sources: RIB
  feature space:
    IPRM: 0x00048000
    Broker: linked, distributed at 3rd priority
  subblocks:
    Replicated from VRF 1
  ifnums:
    GigabitEthernet3(9): 10.20.1.2
  path list 7F890C8E2F20, 7 locks, per-destination, flags 0x69 [shble, rif, rcrsv, hwcn]
    path 7F890FB18F08, share 1/1, type recursive, for IPv4
      recursive via 10.20.1.2[IPv4:1], fib 7F890B609578, 1 terminal fib, v4:1:10.20.1.2/32
      path list 7F890C8E3148, 2 locks, per-destination, flags 0x49 [shble, rif, hwcn]
          path 7F890FB19178, share 1/1, type adjacency prefix, for IPv4
            attached to GigabitEthernet3, IP adj out of GigabitEthernet3, addr 10.20.1.2
7F890FAE4CD8
  output chain:
    IP adj out of GigabitEthernet3, addr 10.20.1.2 7F890FAE4CD8
```

show ip msdp vrf count

To display the number of sources and groups originated in MSDP SA messages and the number of SA messages from an MSDP peer in the SA cache. use the **show ip msdp vrf count** command in privileged EXEC mode.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	This command is supported in Cisco Catalyst SD-WAN

Usage Guidelines

For usage guidelines, see the Cisco IOS XE show ip msdp count command.

Example

The following example displays the number of sources and groups originated in MSDP SA messages and the number of SA messages from an MSDP peer in the SA cache.

```
Device# show ip msdp vrf 1 count
SA State per Peer Counters, <Peer>: <# SA learned>
    10.168.3.11: 1
    10.168.11.15: 0
    10.168.12.12: 0
    10.168.14.14: 0
    10.168.5.24: 0

SA State per ASN Counters, <asn>: <# sources>/<# groups>
    Total entries: 1
    ?: 1/1
```

show ip msdp vrf peer

To display detailed information about Multicast Source Discovery Protocol (MSDP) peers, use the **show ip msdp vrf peer** command in privileged EXEC mode.

Command Modes

Privileged EXEC (#)

Command History

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	This command is supported in Cisco Catalyst SD-WAN

Usage Guidelines

For usage guidelines, see the Cisco IOS XE show ip msdp peer command.

Examples

The following example displays detailed information about Multicast Source Discovery Protocol (MSDP) peers.

```
Device# show ip msdp vrf 1 peer 10.135.250.116
MSDP Peer 10.135.250.116 (?), AS ?
  Connection status:
    State: Up, Resets: 0, Connection source: GigabitEthernet5 (10.168.21.28)
    Uptime(Downtime): 16w4d, Messages sent/received: 169100/169106
    Output messages discarded: 82
    Connection and counters cleared 16w4d    ago
    Peer is member of mesh-group site3
  SA Filtering:
    Input (S,G) filter: sa-filter, route-map: none
    Input RP filter: none, route-map: none
    Output (S,G) filter: none, route-map: none
    Output RP filter: none, route-map: none
  SA-Requests:
    Input filter: none
  Peer ttl threshold: 0
  SAs learned from this peer: 0
  Number of connection transitions to Established state: 1
    Input queue size: 0, Output queue size: 0
  MD5 signature protection on MSDP TCP connection: not enabled
  Message counters:
    RPF Failure count: 0
    SA Messages in/out: 10700/10827
    SA Requests in: 0
    SA Responses out: 0
    Data Packets in/out: 0/10
```

show ip msdp vrf sa-cache

To display the (S,G) state learned from Multicast Source Discovery Protocol (MSDP) peers, use the **show ip msdp vrf sa-cache** command in privileged EXEC mode.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	This command is supported in Cisco Catalyst SD-WAN

Usage Guidelines

For usage guidelines, see the Cisco IOS XE show ip msdp sa-cache command.

Example

The following example displays the (S,G) state learned from Multicast Source Discovery Protocol (MSDP) peers. This command gives information about MSDP SA messages received from the MSDP peer. In the case of Cisco IOS XE Catalyst SD-WAN devices configured for MSDP interworking, the SA message is advertised as OMP source active.

```
Device# show ip msdp vrf 1 sa-cache
MSDP Source-Active Cache - 1 entries
(10.169.1.1, 12.169.1.1), RP 11.41.41.41, AS ?,6d20h/00:05:55, Peer 12.168.3.11
```

show ip msdp vrf summary

To display Multicast Source Discovery Protocol (MSDP) peer status, use the **show ip msdp vrf summary**command in privileged EXEC mode.

Command Modes

Privileged EXEC (#)

Command History

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	This command is supported in Cisco Catalyst SD-WAN

Usage Guidelines

For usage guidelines, see the Cisco IOS XE show ip msdp summary command.

Example

The following example displays Multicast Source Discovery Protocol (MSDP) peer status.

```
Device# show ip msdp vrf 1 summary
MSDP Peer Status Summary
Peer Address     AS    State    Uptime/  Reset SA    Peer Name
                                Downtime Count Count
12.168.3.11      ?     Up       17w6d    0     1     ?
12.168.11.15     ?     Up       17w6d    0     0     ?
12.168.12.12     ?     Up       17w6d    0     0     ?
12.168.14.14     ?     Up       17w6d    0     0     ?
12.168.5.24      ?     Up       17w6d    1     0     ?
```

show ip interface

To display a summary of IP, status and configuration of device interfaces, use the **show ip interface** command in privileged EXEC mode.

show ip interface [**brief**] [*type*] [*number*] [**stats** | **topology** { *WORD* | **all** | **base** } **stats** | **unnumbered** { **detail** }]

Syntax Description

brief	(Optional) Displays brief summary of IP status and configuration.
type	(Optional) Interface Type.
number	(Optional) Interface Number.
stats	(Optional) Shows sum statistics.
topology	(Optional) Topology qualifier for filtering statistics.
WORD	(Optional) Shows the instance topology statistics.
all	(Optional) Shows all topologies statistics.

base	(Optional) Shows base topologies statistics.
stats	(Optional) Shows topology statistics.
unnumbered	(Optional) Displays IP unnumbered status.
detail	(Optional) Displays detailed IP unnumbered status.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

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 about all the interfaces is displayed.

Example

The following example shows how to display interface information on all interfaces.

```
Device# show ip interface

GigabitEthernet0/0/0 is up, line protocol is up
Internet address is 10.10.10.10/24
Broadcast address is 255.255.255.255
Address determined by unknown means
MTU is 1500 bytes
<output truncated>

GigabitEthernet0/0/2 is down, line protocol is down
Internet protocol processing disabled
GigabitEthernet0 is administratively down, line protocol is down
Internet address is 192.168.1.1/24
Broadcast address is 255.255.255.255
Address determined by unknown means
MTU is 1500 bytes
<output truncated>

Dialer1 is up, line protocol is up
Internet protocol processing disabled
Loopback89 is up, line protocol is up
Internet protocol processing disabled
Loopback65528 is up, line protocol is up
Internet address is 192.168.1.1/32
Broadcast address is 255.255.255.255
```

```
Address determined by unknown means
MTU is 1514 bytes
<output truncated>
```

The following example shows how to display interface information on Gigabit Ethernet interface 0/0/0.

```
Device# show ip interface GigabitEthernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
Internet address is 10.10.10.10/24
Broadcast address is 255.255.255.255
Address determined by unknown means
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing Common access list is not set
Outgoing access list is not set
Inbound Common access list is not set
Inbound access list is not set
Proxy ARP is disabled (Globally)
Local Proxy ARP is disabled
Security level is default
Split horizon is enabled
ICMP redirects are never sent
ICMP unreachables are always sent
ICMP mask replies are never sent
IP fast switching is enabled
IP Flow switching is disabled
IP CEF switching is enabled
IP CEF switching turbo vector
IP Null turbo vector
Associated unicast routing topologies:
Topology "base", operation state is UP
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
BGP Policy Mapping is disabled
Input features: MCI Check
IPv4 WCCP Redirect outbound is disabled
IPv4 WCCP Redirect inbound is disabled
IPv4 WCCP Redirect exclude is disabled
```

The following example shows how to display only stats information on Gigabit Ethernet interface 0/0/0.

```
Device# show ip interface GigabitEthernet 0/0/0 stats

GigabitEthernet0/0/0
5 minutes input rate 0 bits/sec, 0 packet/sec,
5 minutes output rate 0 bits/sec, 0 packet/sec,
0 packets input, 0 bytes,
0 packets output, 0 bytes.
```

The following example shows how to display brief summary of IP status and configuration on Gigabit Ethernet interface 0/0/0.

```
Device# show ip interface brief GigabitEthernet 0/0/0

Interface IP-Address OK? Method Status Protocol
GigabitEthernet0/0/0 10.10.10.10 YES other up up
```

The following example shows how to display the number of IP unnumbered status on Gigabit Ethernet interface 0/0/0.

```
Device# show ip interface GigabitEthernet 0/0/0 unnumbered

Number of unnumbered interfaces with polling: 0
```

The following example shows how to display all topologies stats on Gigabit Ethernet interface 0/0/0.

```
Device# show ip interface GigabitEthernet 0/0/0 topology all stats

GigabitEthernet0/0/0
Topology: base
5 minutes input rate 0 bits/sec, 0 packet/sec,
5 minutes output rate 0 bits/sec, 0 packet/sec,
0 packets input, 0 bytes,
0 packets output, 0 bytes.
```

show ip interface brief

To display a summary of IP, status and configuration of device interfaces, use the **show ip interface brief** command in privileged EXEC mode.

show ip interface brief
show ip interface brief [*type*] [*number*] [**stats** | **topology** { *WORD* | **all** | **base** } **stats**]

Syntax Description

None	Brief summary of IP, status and configuration.
type	(Optional) Interface Type.
number	(Optional) Interface Number.
stats	(Optional) Show sum statistics.
topology	(Optional) Topology qualifier for filtering statistics.
WORD	Shows the instance topology statistics.
all	Shows all topologies statistics.
base	Shows base topologies statistics.
stats	Shows topology statistics.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

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.

Example

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   administra
                                                   -tively 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
<output truncated>
```

Table 88: Related Commands

Commands	Description
show interface description	Shows interface status and description.

show ip nat redundancy

To view information about the IP address associated with the Hot Standby Router Protocol (HSRP) redundancy group name, use the **show ip nat redundancy** command in privileged EXEC mode.

show ip nat redundancy

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This command was introduced.

Examples

The following is an example output for the **show ip nat redundancy** command:

```
Device# show ip nat redundancy
IP             Redundancy-Name     ID      Use-count
192.168.0.200  hsrp_lan            0       1
```

The output above shows the IP address associated with the HSRP group name.

For more information on static NAT mapping with HSRP, see the *Cisco SD-WAN NAT Configuration Guide*.

Related Commands

Commands	Description
show ip nat translations	Displays active NAT translations.
show standby	Displays HSRP information.

show ip nat route-dia

To show the number of NAT DIA-enabled routes, use the **show ip nat dia-route** command in privileged EXEC mode.

show ip nat dia-route

Syntax Description

This command has no arguments or keywords.

Command Default

NAT DIA route status information is not displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	This command is supported for Cisco Catalyst SD-WAN.

Examples

The following is a sample output from the **show ip nat dia-route** command:

```
Device# show ip nat route-dia
route add [1] addr [0.0.0.0] vrfid [2] prefix len [0]
route add [1] addr [0.0.0.0] vrfid [4] prefix len [0]
```

show ip nat statistics

To display Network Address Translation (NAT) statistics, use the **show ip nat statistics** command in user EXEC or privileged EXEC mode.

show ip nat statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
16.10	This command was introduced.

Examples

The following is sample output from the **show ip nat statistics** command:

```
Device# show ip nat statistics

Total translations: 2 (0 static, 2 dynamic; 0 extended)
Outside interfaces: Serial0
Inside interfaces: Ethernet1
Hits: 135  Misses: 5
Expired translations: 2
Dynamic mappings:
-- Inside Source
access-list 1 pool net-208 refcount 2
 pool net-208: netmask 255.255.255.240
        start 172.16.233.208 end 172.16.233.221
        type generic, total addresses 14, allocated 2 (14%), misses 0
```

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

Table 89: show ip nat statistics Field Descriptions

Field	Description
Total translations	Number of translations active in the system. This number is incremented each time a translation is created and is decremented each time a translation is cleared or times out.
Outside interfaces	List of interfaces marked as outside with the **ip nat outside** command.
Inside interfaces	List of interfaces marked as inside with the **ip nat inside** command.
Hits	Number of times the software does a translations table lookup and finds an entry.
Misses	Number of times the software does a translations table lookup, fails to find an entry, and must try to create one.
Expired translations	Cumulative count of translations that have expired since the router was booted.
Dynamic mappings	Indicates that the information that follows is about dynamic mappings.
Inside Source	Indicates that the information that follows is about an inside source translation.
access-list	Access list number being used for the translation.
pool	Name of the pool (in this case, net-208).
refcount	Number of translations using this pool.
netmask	IP network mask being used in the pool.
start	Starting IP address in the pool range.

Field	Description
end	Ending IP address in the pool range.
type	Type of pool. Possible types are generic or rotary.
total addresses	Number of addresses in the pool available for translation.
allocated	Number of addresses being used.
misses	Number of failed allocations from the pool.

show ip nat translations

To display active Network Address Translation (NAT) translations, use the **show ip nat translations** command in privilege EXEC mode.

show ip nat translations [**inside** *global-ip*] [**outside** *local-ip*] [**icmp**] [**tcp**] [**udp**] [**verbose**] [**vrf** *vrf-name*]

Syntax Description

icmp	(Optional) Displays Internet Control Message Protocol (ICMP) entries.
inside *global-ip*	(Optional) Displays entries for only a specific inside global IP address.
outside *local-ip*	(Optional) Displays entries for only a specific outside local IP address.
tcp	(Optional) Displays TCP protocol entries.
udp	(Optional) Displays User Datagram Protocol (UDP) entries.
verbose	(Optional) Displays additional information for each translation table entry, including how long ago the entry was created and used.
vrf *vrf-name*	(Optional) Displays VPN routing and forwarding (VRF) traffic-related information.

Command Modes

Privilege EXEC (#)

Command History

Release	Modification
16.10	This command was introduced.

Examples

The following is sample output from the **show ip nat translations** command. Without overloading, two inside hosts are exchanging packets with some number of outside hosts.

```
Device# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
--- 10.69.233.209     192.168.1.95       ---                ---
--- 10.69.233.210     192.168.1.89       ---                --
```

With overloading, a translation for a Domain Name Server (DNS) transaction is still active, and translations for two Telnet sessions (from two different hosts) are also active. Note that two different inside hosts appear on the outside with a single IP address.

```
Device# show ip nat translations
Pro Inside global        Inside local       Outside local      Outside global
udp 10.69.233.209:1220  192.168.1.95:1220  172.16.2.132:53    172.16.2.132:53
tcp 10.69.233.209:11012 192.168.1.89:11012 172.16.1.220:23    172.16.1.220:23
tcp 10.69.233.209:1067  192.168.1.95:1067  172.16.1.161:23    172.16.1.161:23
```

The following is sample output that includes the **verbose** keyword:

```
Device# show ip nat translations verbose
Pro Inside global        Inside local       Outside local      Outside global
udp 172.16.233.209:1220  192.168.1.95:1220  172.16.2.132:53    172.16.2.132:53
        create 00:00:02, use 00:00:00, flags: extended
tcp 172.16.233.209:11012 192.168.1.89:11012 172.16.1.220:23    172.16.1.220:23
        create 00:01:13, use 00:00:50, flags: extended
tcp 172.16.233.209:1067  192.168.1.95:1067  172.16.1.161:23    172.16.1.161:23
        create 00:00:02, use 00:00:00, flags: extended
```

The following is sample output that includes the **vrf** keyword:

```
Device# show ip nat translations vrf
abc
Pro Inside global      Inside local       Outside local      Outside global
--- 10.2.2.1            192.168.121.113    ---                ---
--- 10.2.2.2            192.168.122.49     ---                ---
--- 10.2.2.11           192.168.11.1       ---                ---
--- 10.2.2.12           192.168.11.3       ---                ---
--- 10.2.2.13           172.16.5.20        ---                ---
Pro Inside global      Inside local       Outside local      Outside global
--- 10.2.2.3            192.168.121.113    ---                ---
--- 10.2.2.4            192.168.22.49      ---                ---
```

The following is sample output that includes the **esp** keyword:

```
Device# show ip nat translations esp

Pro Inside global         Inside local          Outside local         Outside global
esp 192.168.22.40:0      192.168.122.20:0     192.168.22.20:0      192.168.22.20:28726CD9

esp 192.168.22.40:0       192.168.122.20:2E59EEF5 192.168.22.20:0     192.168.22.20:0
```

The following is sample output that includes the **esp** and **verbose** keywords:

```
Device# show ip nat translation esp verbose

Pro Inside global         Inside local          Outside local         Outside global
esp 192.168.22.40:0      192.168.122.20:0     192.168.22.20:0      192.168.22.20:28726CD9

    create 00:00:00, use 00:00:00,
    flags:
extended, 0x100000, use_count:1, entry-id:192, lc_entries:0
esp 192.168.22.40:0       192.168.122.20:2E59EEF5 192.168.22.20:0     192.168.22.20:0
    create 00:00:00, use 00:00:00, left 00:04:59, Map-Id(In):20,
    flags:
extended, use_count:0, entry-id:191, lc_entries:0
```

The following is sample output that includes the **inside**keyword:

```
Device# show ip nat translations inside 10.69.233.209
Pro Inside global        Inside local       Outside local      Outside global
udp 10.69.233.209:1220  192.168.1.95:1220  172.16.2.132:53    172.16.2.132:53
```

The following is sample output when NAT that includes the **inside**keyword:

```
Device# show ip nat translations inside 10.69.233.209
Pro Inside global        Inside local       Outside local      Outside global
udp 10.69.233.209:1220  192.168.1.95:1220  172.16.2.132:53    172.16.2.132:53
```

The following is a sample output that displays information about NAT port parity and conservation:

```
Device# show ip nat translations
Pro  Inside global         Inside local          Outside local         Outside global
udp  200.200.0.100:5066    100.100.0.56:5066     200.200.0.56:5060     200.200.0.56:5060
udp  200.200.0.100:1025    100.100.0.57:10001    200.200.0.57:10001    200.200.0.57:10001
udp  200.200.0.100:10000   100.100.0.56:10000    200.200.0.56:10000    200.200.0.56:10000
udp  200.200.0.100:1024    100.100.0.57:10000    200.200.0.57:10000    200.200.0.57:10000
udp  200.200.0.100:10001   100.100.0.56:10001    200.200.0.56:10001    200.200.0.56:10001
udp  200.200.0.100:9985    100.100.0.57:5066     200.200.0.57:5060     200.200.0.57:5060
Total number of translations: 6
```

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

Table 90: show ip nat translations Field Descriptions

Field	Description
Pro	Protocol of the port identifying the address.
Inside global	The legitimate IP address that represents one or more inside local IP addresses to the outside world.
Inside local	The IP address assigned to a host on the inside network; probably not a legitimate address assigned by the Network Interface Card (NIC) or service provider.
Outside local	IP address of an outside host as it appears to the inside network; probably not a legitimate address assigned by the NIC or service provider.
Outside global	The IP address assigned to a host on the outside network by its owner.
create	How long ago the entry was created (in hours:minutes:seconds).
use	How long ago the entry was last used (in hours:minutes:seconds).
flags	Indication of the type of translation. Possible flags are: • extended--Extended translation • static--Static translation • destination--Rotary translation • outside--Outside translation • timing out--Translation will no longer be used, due to a TCP finish (FIN) or reset (RST) flag.

show ip nat status

To view the status of Network Address Translation (NAT), use the command **show ip nat translations** in user EXEC or privileged EXEC mode. This command displays all active NAT translations including details like inside source IP, translated outside IP, protocol, and port information

show running nat [**all** | **route** | **pool** | **port** | **cpu** | **memory** | **GK** | **packet**]

Syntax Description

all	Displays all information about all NAT statistics and status.
route	Displays NAT routing information.
pool	Displays information about NAT address pools.
port	Provides details on port usage for NAT translations.
cpu	Displays CPU utilization related to NAT processes.
memory	Displays memory usage by NAT processes.
GK	Displays specific information to Gatekeeper NAT.
packet	Provides statistics on packets processed by NAT.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.18.1a	This command was introduced.

Usage Guidelines

Example

The **show ip nat status all** command displays all the output of **show ip nat status** sub commands. The following example shows routing table for NAT enabled VRFs:

```
Device# show ip nat status route
Routing Table: 1
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected
```

```
Gateway of last resort is not set
```

show running nat

To display Network Address Translation (NAT) configuration details, use the **show running nat** command in user EXEC or privileged EXEC mode.

show running nat [**all** | **interface** | **policy** | **acl** | **static** | **dynamic**]

Syntax Description

all	Displays all NAT configurations, including static and dynamic rules across all interfaces.
interface	Displays NAT rules specifically applied to a particular network interface.
policy	Displays only the NAT policies configured on the device, including source and destination translation rules.
acl	Displays NAT rules associated with a specific access control list (ACL).
static	Displays only the static NAT rules configured on the device.
dynamic	Displays only the dynamic NAT rules, where the translated address can change based on available IP addresses in a pool.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.18.1a	This command was introduced.

Usage Guidelines

Example

The **show running nat all** command displays all the output of **show running nat** sub commands. The following example shows how to display the NAT policies configured on the device:

```
Device# show running nat policy
from-vsmart data-policy ssn_policy
 direction all
 vpn-list ssn_vpn_list
  sequence 101
   match
    source-ip 192.168.0.0/16
    protocol  1
   action accept
    nat pool 1
  default-action accept
from-vsmart lists vpn-list ssn_vpn_list
 vpn 1
```

show ip pim bsr-router

To view information about a bootstrap router (BSR), use the **show ip pim bsr-router** command in privileged EXEC mode.

show ip pim [**vrf** *vrf-name*] **bsr-router**

Syntax Description

vrf *vrf-name*	(Optional) Displays information about a BSR associated with the multicast virtual private network's (MVPN) multicast routing and forwarding instance (MVRF) specified for the *vrf-name* argument.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE show ip pim bsr-router command.

Examples

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 rp

To view information about the mappings for the PIM group to the active rendezvous points (RPs), use the **show ip pim rp** command in privileged EXEC mode.

show ip pim [**vrf** *vrf-name*] **rp mapping** [*rp-address*]

Syntax Description

vrf *vrf-name*	(Optional) Configures the router to announce its candidacy as a BSR for the multicast virtual private network's (MVPN) multicast routing and forwarding instance (MVRF) specified for the *vrf-name* argument.
rp mapping *rp-address*	(Optional) Displays information about the mappings for the PIM group to the active RPs.

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines Use this command to view information about the mappings for the PIM group to the active RPs.

Examples The following is sample output from the **show ip pim vrf rp mapping** command:

```
Device# show ip pim vrf 1 rp mapping
PIM Group-to-RP Mappings
This system is a candidate RP (v2)
This system is the Bootstrap Router (v2)

Group(s) 224.0.0.0/4
RP 10.1.10.2 (?), v2
Info source: 10.1.10.2 (?), via bootstrap, priority 0, holdtime 75
Uptime: 15:46:47, expires: 00:00:57
Group(s) 225.0.0.0/8
RP 10.1.10.2 (?), v2
Info source: 10.1.10.2 (?), via bootstrap, priority 0, holdtime 75
Uptime: 15:46:47, expires: 00:00:57
RP 10.1.10.1 (?), v2
Info source: 10.1.10.1 (?), via bootstrap, priority 10, holdtime 75
Uptime: 15:45:45, expires: 00:00:59
Group(s) 226.0.0.0/8
RP 10.1.10.2 (?), v2
Info source: 10.1.10.2 (?), via bootstrap, priority 0, holdtime 75
Uptime: 15:46:55, expires: 00:00:49
RP 10.1.10.1 (?), v2
Info source: 10.1.10.1 (?), via bootstrap, priority 10, holdtime 75
Uptime: 15:46:02, expires: 00:01:09
Group(s) 227.0.0.0/8
RP 10.1.10.2 (?), v2
Info source: 10.1.10.2 (?), via bootstrap, priority 0, holdtime 75
Uptime: 15:47:13, expires: 00:00:59
RP 10.1.10.1 (?), v2
Info source: 10.1.10.1 (?), via bootstrap, priority 10, holdtime 75
Uptime: 15:46:20, expires: 00:00:53
Group(s) 228.0.0.0/8
RP 10.1.10.2 (?), v2
Info source: 10.1.10.2 (?), via bootstrap, priority 0, holdtime 75
Uptime: 15:47:31, expires: 00:01:13
```

show ip protocols

To display the parameters and the current state of the active routing protocol process, use the **show ip protocols** command in privileged EXEC mode.

show ip protocols [**multicast** | **summary** | **topology** *topology-name* | **vrf** *vrf-name* | | [**append** | **begin** | **count** | **exclude** | **format** | **include** | **redirect** | **section** | **tee**]]

Syntax Description

multicast	(Optional) Displays multicast global information.
topology*topology-name*	(Optional) Displays protocols for a topology instance.
summary	(Optional) Displays summary information.
vrf*vrf-name*	(Optional) Displays protocols for a VPN Routing/Forwarding instance.
|	(Optional) Displays information for the specified output modifiers: • append: Append redirected output to URL (URLs supporting append operation only). • begin: Begin with the line that matches. • count: Count number of lines which match regexp. • exclude: Exclude lines that match. • format: Format the output using the specified spec file. • include: Include lines that match. • redirect: Redirect output to URL. • section: Filter a section of output. • tee: Copy output to URL.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE show ip protocols command.

Examples

The following sample output from the **showipprotocols** command shows section of RIP:

```
Device# show ip protocols | sec rip
Routing Protocol is "rip"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Sending updates every 30 seconds, next due in 19 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Redistributing: rip
  Neighbor(s):
    41.1.1.2
  Default version control: send version 2, receive version 2
```

```
  Interface                         Send  Recv  Triggered RIP  Key-chain
  GigabitEthernet1                  2     2          No        none
  Loopback10                        2     2          No        none
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
  41.0.0.0
Routing Information Sources:
  Gateway         Distance      Last Update
  41.1.1.2             120      00:00:15
Distance: (default is 120)
```

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

Table 91: show ip protocols Field Descriptions

Field	Description
Routing Protocol is...	Name and autonomous system number of the currently running routing protocol.
Outgoing update filter list for all interfaces...	Indicates whether a filter for outgoing routing updates has been specified with the **distribute-listout** command.
Incoming update filter list for all interfaces...	Indicates whether a filter for incoming routing updates has been specified with the **distribute-listin** command.
Redistributing:	Indicates whether route redistribution has been enabled with the **redistribute** command.
Distance	Internal and external administrative distance. Internal distance is the degree of preference given to RIP internal routes. External distance is the degree of preference given to RIP external routes.
Maximum path	Maximum number of parallel routes that the RIP can support.
Maximum hopcount	Maximum hop count (in decimal).
Maximum metric variance	Metric variance used to find feasible paths for a route.
Automatic Summarization	Indicates whether route summarization has been enabled with the **auto-summary** command.
Routing for Networks:	Networks for which the routing process is currently injecting routes.
Routing Information Sources:	Lists all the routing sources that the Cisco IOS software is using to build its routing table. The following is displayed for each source: • IP address • Administrative distance • Time the last update was received from this source

show ip rip database

To display summary address entries in the Routing Information Protocol (RIP) routing database, if relevant routes are being summarized based upon a summary address, use the **show ip rip database** command in privileged EXEC mode.

show ip rip database [*ip-address mask* | **vrf** *vrf-id*]

Syntax Description

ip-address	(Optional) Specifies IP address (network) for which routing information is displayed.
mask	(Optional) Specifies argument for the subnet mask. The subnet mask must also be specified if the IP address argument is entered.
vrf	(Optional) Specifies VPN routing or forwarding instance.
vrf-id	VPN routing or forwarding instance name.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE show ip rip database command.

Examples

The following is a sample output from the **show ip rip database** command displaying the contents of the RIP private database:

```
Device# show ip rip database vrf 1
10.0.0.1/8 auto-summary
10.1.1.1/32 directly connected, Loopback1
10.2.2.2/8 auto-summary
10.2.2.2/8
[1] via 10.10.10.2, 00:00:29, GigabitEthernet 1/0/1
10.20.20.20/32
[1] via 10.10.10.2, 00:00:03, GigabitEthernet 1/0/1
10.0.0.1/8 auto-summary
10.10.10.0/24 directly connected, GigabitEthernet 1/0/1
```

The following is a sample output from the **show ip rip database** command displaying a summary address entry for route 10.11.0.0/16, with a child route active:

```
Device# show ip rip database
10.11.0.0/16    auto-summary
10.11.0.0/16
[1] via 172.16.1.2, 00:00:00, GigabitEthernet1
```

The table below describes the fields in the display.

Table 92: show ip rip database command Field Descriptions

Field	Description
10.11.0.0/16 auto-summary	Specifies summary address entry.
10.11.0.0/16 [1] via 172.16.1.2, 00:00:00, GigabitEthernet1	RIP is used to discover the destination 10.11.0.0/16. There is a source advertising it. 172.16.1.2 through GigabitEthernet1.

show ip rip neighbors

To display the Routing Information Protocol (RIP) neighbors for which Bidirectional Forwarding Detection (BFD) sessions are created, use the **show ip rip neighbors** command in privileged EXEC mode.

show ip rip neighbors

Syntax Description

This command has no argument or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE show ip rip neighbors command.

Examples

The following is a sample output from the **show ip rip neighbors** command displaying RIP BFD neighbors:

```
Device# show ip rip neighbors
BFD sessions created for the RIP neighbors
Neighbor      Interface         SessionHandle
10.10.10.2    GigabitEthernet1    1
```

The table below describes the significant fields shown in the display:

Table 93: show ip rip neighbors command Field Descriptions

Field	Description
Neighbor	Specifies neighboring router for which BFD sessions are created.
Interface	Specifies the interface type of the neigboring router.
SessionHandle	Specifies the unique session handle number to track the neighbor. The BFD system provides this number.

show ip route

To display contents of the routing table, use the **show ip route** command in user EXEC or privileged EXEC mode.

show ip route [*ip-address* [**repair-paths** | **next-hop-override** [**dhcp**] | *mask* [**longer-prefixes**]] | *protocol* [*process-id*] | **list** [*access-list-number access-list-name*] | **static download** | **update-queue**]

Syntax Description

ip-address	(Optional) IP address for which routing information should be displayed.
repair-paths	(Optional) Displays the repair paths.
next-hop-override	(Optional) Displays the Next Hop Resolution Protocol (NHRP) next-hop overrides that are associated with a particular route and the corresponding default next hops.
dhcp	(Optional) Displays routes added by the Dynamic Host Configuration Protocol (DHCP) server.
mask	(Optional) Subnet mask.
longer-prefixes	(Optional) Displays output for longer prefix entries.
protocol	(Optional) The name of a routing protocol or the keyword **connected**, **mobile**, **static**, or **summary**. If you specify a routing protocol, use one of the following keywords: **bgp**, **eigrp**, **hello**, **isis**, **odr**, **ospf**, **nhrp**, or **rip**.
process-id	(Optional) Number used to identify a process of the specified protocol.
list	(Optional) Filters output by an access list name or number.
access-list-number	(Optional) Access list number.
access-list-name	(Optional) Access list name.
static	(Optional) Displays static routes.
download	(Optional) Displays routes installed using the authentication, authorization, and accounting (AAA) route download function. This keyword is used only when AAA is configured.
update-queue	(Optional) Displays Routing Information Base (RIB) queue updates.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
17.3.1	This command was introduced.

The following is sample output from the **show iproute** command when an IP address is not specified:

```
Device# show ip route

Codes: R - RIP derived, O - OSPF derived,
       C - connected, S - static, B - BGP derived,
       * - candidate default route, IA - OSPF inter area route,
       i - IS-IS derived, ia - IS-IS, U - per-user static route,
       o - on-demand routing, M - mobile, P - periodic downloaded static route,
       D - EIGRP, EX - EIGRP external, E1 - OSPF external type 1 route,
       E2 - OSPF external type 2 route, N1 - OSPF NSSA external type 1 route,
       N2 - OSPF NSSA external type 2 route
Gateway of last resort is 10.119.254.240 to network 10.140.0.0
O E2 10.110.0.0 [160/5] via 10.119.254.6, 0:01:00, Ethernet2
E    10.67.10.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
O E2 10.68.132.0 [160/5] via 10.119.254.6, 0:00:59, Ethernet2
O E2 10.130.0.0 [160/5] via 10.119.254.6, 0:00:59, Ethernet2
E    10.128.0.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E    10.129.0.0 [200/129] via 10.119.254.240, 0:02:22, Ethernet2
E    10.65.129.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E    10.10.0.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E    10.75.139.0 [200/129] via 10.119.254.240, 0:02:23, Ethernet2
E    10.16.208.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E    10.84.148.0 [200/129] via 10.119.254.240, 0:02:23, Ethernet2
E    10.31.223.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E    10.44.236.0 [200/129] via 10.119.254.240, 0:02:23, Ethernet2
E    10.141.0.0 [200/129] via 10.119.254.240, 0:02:22, Ethernet2
E    10.140.0.0 [200/129] via 10.119.254.240, 0:02:23, Ethernet2
```

The following sample output from the **show ip routes** command includes routes learned from IS-IS Level 2:

```
Device# show ip route

Codes: R - RIP derived, O - OSPF derived,
       C - connected, S - static, B - BGP derived,
       * - candidate default route, IA - OSPF inter area route,
       i - IS-IS derived, ia - IS-IS, U - per-user static route,
       o - on-demand routing, M - mobile, P - periodic downloaded static route,
       D - EIGRP, EX - EIGRP external, E1 - OSPF external type 1 route,
       E2 - OSPF external type 2 route, N1 - OSPF NSSA external type 1 route,
       N2 - OSPF NSSA external type 2 route
Gateway of last resort is not set
     10.89.0.0 is subnetted (mask is 255.255.255.0), 3 subnets
C       10.89.64.0 255.255.255.0 is possibly down,
          routing via 0.0.0.0, Ethernet0
i L2    10.89.67.0 [115/20] via 10.89.64.240, 0:00:12, Ethernet0
i L2    10.89.66.0 [115/20] via 10.89.64.240, 0:00:12, Ethernet0
```

The following is sample output from the **show ip route** *ip-address mask* **longer-prefixes** command. When this keyword is included, the address-mask pair becomes the prefix, and any address that matches that prefix is displayed. Therefore, multiple addresses are displayed. The logical AND operation is performed on the source address 0.0.0.0 and the mask 0.0.0.0, resulting in 0.0.0.0. Each destination in the routing table is also logically ANDed with the mask and compared with 0.0.0.0. Any destinations that fall into that range are displayed in the output.

```
Device# show ip route 0.0.0.0 0.0.0.0 longer-prefixes

Codes: R - RIP derived, O - OSPF derived,
       C - connected, S - static, B - BGP derived,
```

```
       * - candidate default route, IA - OSPF inter area route,
       i - IS-IS derived, ia - IS-IS, U - per-user static route,
       o - on-demand routing, M - mobile, P - periodic downloaded static route,
       D - EIGRP, EX - EIGRP external, E1 - OSPF external type 1 route,
       E2 - OSPF external type 2 route, N1 - OSPF NSSA external type 1 route,
       N2 - OSPF NSSA external type 2 route

Gateway of last resort is not set

S    10.134.0.0 is directly connected, Ethernet0
S    10.10.0.0 is directly connected, Ethernet0
S    10.129.0.0 is directly connected, Ethernet0
S    10.128.0.0 is directly connected, Ethernet0
S    10.49.246.0 is directly connected, Ethernet0
S    10.160.97.0 is directly connected, Ethernet0
S    10.153.88.0 is directly connected, Ethernet0
S    10.76.141.0 is directly connected, Ethernet0
S    10.75.138.0 is directly connected, Ethernet0
S    10.44.237.0 is directly connected, Ethernet0
S    10.31.222.0 is directly connected, Ethernet0
S    10.16.209.0 is directly connected, Ethernet0
S    10.145.0.0 is directly connected, Ethernet0
S    10.141.0.0 is directly connected, Ethernet0
S    10.138.0.0 is directly connected, Ethernet0
S    10.128.0.0 is directly connected, Ethernet0
     10.19.0.0 255.255.255.0 is subnetted, 1 subnets
C       10.19.64.0 is directly connected, Ethernet0
     10.69.0.0 is variably subnetted, 2 subnets, 2 masks
C       10.69.232.32 255.255.255.240 is directly connected, Ethernet0
S       10.69.0.0 255.255.0.0 is directly connected, Ethernet0
```

The following sample outputs from the **show ip route** command display all downloaded static routes. A “p” indicates that these routes were installed using the AAA route download function.

```
Device# show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR, P - periodic downloaded static route
       T - traffic engineered route

Gateway of last resort is 172.16.17.1 to network 10.0.0.0

        172.31.0.0/32 is subnetted, 1 subnets
P       172.31.229.41 is directly connected, Dialer1 0.0.0.0/0 is subnetted, 3 subnets
P       10.1.1.0 [200/0] via 172.31.229.41, Dialer1
P       10.1.3.0 [200/0] via 172.31.229.41, Dialer1
P       10.1.2.0 [200/0] via 172.31.229.41, Dialer1

Device# show ip route static

     172.16.4.0/8 is variably subnetted, 2 subnets, 2 masks
P       172.16.1.1/32 is directly connected, BRI0
P       172.16.4.0/8 [1/0] via 10.1.1.1, BRI0
S    172.31.0.0/16 [1/0] via 172.16.114.65, Ethernet0
S    0.0.0.0/0 is directly connected, BRI0
P    0.0.0.0/0 is directly connected, BRI0
     172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
S       172.16.114.201/32 is directly connected, BRI0
S       172.16.114.205/32 is directly connected, BRI0
```

```
S       172.16.114.174/32 is directly connected, BRI0
S       172.16.114.12/32 is directly connected, BRI0
P    0.0.0.0/8 is directly connected, BRI0
P    0.0.0.0/16 is directly connected, BRI0
P    10.2.2.0/24 is directly connected, BRI0
S*   0.0.0.0/0 [1/0] via 172.16.114.65, Ethernet0
S    172.16.0.0/16 [1/0] via 172.16.114.65, Ethernet0
```

The following sample output from the **show ip route static download** command displays all active and inactive routes installed using the AAA route download function:

```
Device# show ip route static download

Connectivity: A - Active, I - Inactive

A     10.10.0.0 255.0.0.0 BRI0
A     10.11.0.0 255.0.0.0 BRI0
A     10.12.0.0 255.0.0.0 BRI0
A     10.13.0.0 255.0.0.0 BRI0
I     10.20.0.0 255.0.0.0 172.21.1.1
I     10.22.0.0 255.0.0.0 Serial0
I     10.30.0.0 255.0.0.0 Serial0
I     10.31.0.0 255.0.0.0 Serial1
I     10.32.0.0 255.0.0.0 Serial1
A     10.34.0.0 255.0.0.0 192.168.1.1
A     10.36.1.1 255.255.255.255 BRI0 200 name remote1
I     10.38.1.9 255.255.255.0 192.168.69.1
```

The following sample outputs from the **show ip route nhrp** command display shortcut switching on the tunnel interface:

```
Device# show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
Gateway of last resort is not set
0.0.0.0/16 is variably subnetted, 3 subnets, 2 masks
C       10.1.1.0/24 is directly connected, Tunnel0
C       172.16.22.0 is directly connected, Ethernet1/0
H       172.16.99.0 [250/1] via 10.1.1.99, 00:11:43, Tunnel0
     10.11.0.0/24 is subnetted, 1 subnets
C       10.11.11.0 is directly connected, Ethernet0/0

Device# show ip route nhrp

H       172.16.99.0 [250/1] via 10.1.1.99, 00:11:43, Tunnel0
```

The following are sample outputs from the **show ip route** command when the **next-hop-override** keyword is used. When this keyword is included, the NHRP next-hop overrides that are associated with a particular route and the corresponding default next hops are displayed.

```
==============================================================
1) Initial configuration
==============================================================

Device# show ip route
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
       + - replicated route

Gateway of last resort is not set
      10.2.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        10.2.1.0/24 is directly connected, Loopback1
L        10.2.1.1/32 is directly connected, Loopback1
      0.0.0.0/24 is subnetted, 1 subnets
S        10.10.10.0 is directly connected, Tunnel0
      10.11.0.0/24 is subnetted, 1 subnets
S        10.11.11.0 is directly connected, Ethernet0/0

Device# show ip route next-hop-override

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
       + - replicated route

Gateway of last resort is not set
      10.2.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        10.2.1.0/24 is directly connected, Loopback1
L        10.2.1.1/32 is directly connected, Loopback1
      10.0.0.0/24 is subnetted, 1 subnets
S        10.10.10.0 is directly connected, Tunnel0
      10.11.0.0/24 is subnetted, 1 subnets
S        10.11.11.0 is directly connected, Ethernet0/0

Device# show ip cef

Prefix               Next Hop             Interface
.
.
.
10.2.1.255/32         receive              Loopback1
10.10.10.0/24        attached             Tunnel0  <<<<<<<<
10.11.11.0/24        attached             Ethernet0/0
172.16.0.0/12          drop
.
.
.
==============================================================
2) Add a next-hop override
   address = 10.10.10.0
   mask = 255.255.255.0
   gateway = 10.1.1.1
   interface = Tunnel0
==============================================================

Device# show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
       + - replicated route

Gateway of last resort is not set
      10.2.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        10.2.1.0/24 is directly connected, Loopback1
L        10.2.1.1/32 is directly connected, Loopback1
      10.0.0.0/24 is subnetted, 1 subnets

S        10.10.10.0 is directly connected, Tunnel0
      10.11.0.0/24 is subnetted, 1 subnets
S        10.11.11.0 is directly connected, Ethernet0/0

Device# show ip route next-hop-override

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
       + - replicated route

Gateway of last resort is not set
      10.2.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        10.2.1.0/24 is directly connected, Loopback1
L        10.2.1.1/32 is directly connected, Loopback1
      10.0.0.0/24 is subnetted, 1 subnets

S        10.10.10.0 is directly connected, Tunnel0
                  [NHO][1/0] via 10.1.1.1, Tunnel0
      10.11.0.0/24 is subnetted, 1 subnets
S        10.11.11.0 is directly connected, Ethernet0/0

Device# show ip cef

Prefix               Next Hop             Interface
.
.
.
10.2.1.255/32         receive              Loopback110.10.10.0/24

10.10.10.0/24       10.1.1.1             Tunnel0

10.11.11.0/24       attached            Ethernet0/0
10.12.0.0/16 drop
.
.
.
============================================================
3) Delete a next-hop override
   address = 10.10.10.0
   mask = 255.255.255.0
   gateway = 10.11.1.1
   interface = Tunnel0
============================================================

Device# show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
```

```
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
       + - replicated route

Gateway of last resort is not set
      10.2.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        10.2.1.0/24 is directly connected, Loopback1
L        10.2.1.1/32 is directly connected, Loopback1
      10.0.0.0/24 is subnetted, 1 subnets
S        10.10.10.0 is directly connected, Tunnel0
      10.11.0.0/24 is subnetted, 1 subnets
S        10.11.11.0 is directly connected, Ethernet0/0

Device# show ip route next-hop-override

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
       + - replicated route

Gateway of last resort is not set
      10.2.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        10.2.1.0/24 is directly connected, Loopback1
L        10.2.1.1/32 is directly connected, Loopback1
      10.0.0.0/24 is subnetted, 1 subnets
S        10.10.10.0 is directly connected, Tunnel0
      10.11.0.0/24 is subnetted, 1 subnets
S        10.11.11.0 is directly connected, Ethernet0/0

Device# show ip cef

Prefix               Next Hop             Interface
.
.
.
10.2.1.255/32         receive              Loopback110.10.10.0/24

10.10.10.0/24        attached             Tunnel0
10.11.11.0/24        attached             Ethernet0/0
10.120.0.0/16 drop
.
.
.
```

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

Table 94: show ip route Field Descriptions

Field	Description
Codes (Protocol)	Indicates the protocol that derived the route. It can be one of the following values: • B—BGP derived • C—Connected • D—Enhanced Interior Gateway Routing Protocol (EIGRP) • EX—EIGRP external • H—NHRP • i—IS-IS derived • ia—IS-IS • L—Local • M—Mobile • o—On-demand routing • O—Open Shortest Path First (OSPF) derived • P—Periodic downloaded static route • R—Routing Information Protocol (RIP) derived • S—Static • U—Per-user static route • +—Replicated route
Codes (Type)	Type of route. It can be one of the following values: • *—Indicates the last path used when a packet was forwarded. This information is specific to nonfast-switched packets. • E1—OSPF external type 1 route • E2—OSPF external type 2 route • IA—OSPF interarea route • L1—IS-IS Level 1 route • L2—IS-IS Level 2 route • N1—OSPF not-so-stubby area (NSSA) external type 1 route • N2—OSPF NSSA external type 2 route
10.110.0.0	Indicates the address of the remote network.

Field	Description
[160/5]	The first number in brackets is the administrative distance of the information source; the second number is the metric for the route.
via 10.119.254.6	Specifies the address of the next device to the remote network.
0:01:00	Specifies the last time the route was updated (in hours:minutes:seconds).
Ethernet2	Specifies the interface through which the specified network can be reached.

The following is sample output from the **show ip route** command when an IP address is specified:

```
Device# show ip route 0.0.0.0

Routing entry for 0.0.0.0/0
    Known via "isis", distance 115, metric 20, type level-1
    Redistributing via isis
    Last update from 10.191.255.251 on Fddi1/0, 00:00:13 ago
    Routing Descriptor Blocks:
    * 10.22.22.2, from 10.191.255.247, via Serial2/3
       Route metric is 20, traffic share count is 1
       10.191.255.251, from 10.191.255.247, via Fddi1/0
       Route metric is 20, traffic share count is 1
```

When an IS-IS router advertises its link-state information, the router includes one of its IP addresses to be used as the originator IP address. When other routers calculate IP routes, they store the originator IP address with each route in the routing table.

The preceding example shows the output from the **show ip route** command for an IP route generated by IS-IS. Each path that is shown under the Routing Descriptor Blocks report displays two IP addresses. The first address (10.22.22.2) is the next-hop address. The second is the originator IP address from the advertising IS-IS router. This address helps you determine the origin of a particular IP route in your network. In the preceding example, the route to 0.0.0.0/0 was originated by a device with IP address 10.191.255.247.

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

Table 95: show ip route with IP Address Field Descriptions

Field	Description
Routing entry for 0.0.0.0/0	Network number and mask.
Known via...	Indicates how the route was derived.
Redistributing via...	Indicates the redistribution protocol.
Last update from 10.191.255.251	Indicates the IP address of the router that is the next hop to the remote network and the interface on which the last update arrived.
Routing Descriptor Blocks	Displays the next-hop IP address followed by the information source.
Route metric	This value is the best metric for this Routing Descriptor Block.
traffic share count	Indicates the number of packets transmitted over various routes.

The following sample output from the **show ip route** command displays the tag applied to the route 10.22.0.0/16. You must specify an IP prefix to see the tag value. The fields in the display are self-explanatory.

```
Device# show ip route 10.22.0.0

Routing entry for 10.22.0.0/16
  Known via "isis", distance 115, metric 12
  Tag 120, type level-1
  Redistributing via isis
  Last update from 172.19.170.12 on Ethernet2, 01:29:13 ago
  Routing Descriptor Blocks:
    * 172.19.170.12, from 10.3.3.3, via Ethernet2
        Route metric is 12, traffic share count is 1
        Route tag 120
```

The following example shows that IP route 10.8.8.0 is directly connected to the Internet and is the next-hop (option 3) default gateway. Routes 10.1.1.1 [1/0], 10.3.2.1 [24/0], and 172.16.2.2 [1/0] are static, and route 0.0.0.0/0 is a default route candidate. The fields in the display are self-explanatory.

```
Device# show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
Gateway of last resort is 10.0.19.14 to network 0.0.0.0
10.0.0.0/24 is subnetted, 1 subnets
C 10.8.8.0 is directly connected, Ethernet1
  10.0.0.0/32 is subnetted, 1 subnets
S 10.1.1.1 [1/0] via 10.8.8.1
  10.0.0.0/32 is subnetted, 1 subnets
S 10.3.2.1 [24/0] via 10.8.8.1
  172.16.0.0/32 is subnetted, 1 subnets
S 172.16.2.2 [1/0] via 10.8.8.1
  10.0.0.0/28 is subnetted, 1 subnets
C 10.0.19.0 is directly connected, Ethernet0
  10.0.0.0/24 is subnetted, 1 subnets
C 10.15.15.0 is directly connected, Loopback0
S* 10.0.0.0/0 [1/0] via 10.0.19.14
```

The following sample output from the **show ip route repair-paths** command shows repair paths marked with the tag [RPR]. The fields in the display are self-explanatory:

```
Device# show ip route repair-paths

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
       + - replicated route, % - next hop override

Gateway of last resort is not set
```

```
      10.0.0.0/32 is subnetted, 3 subnets
C        10.1.1.1 is directly connected, Loopback0
B        10.2.2.2 [200/0] via 172.16.1.2, 00:31:07
                  [RPR][200/0] via 192.168.1.2, 00:31:07
B        10.9.9.9 [20/0] via 192.168.1.2, 00:29:45
                  [RPR][20/0] via 192.168.3.2, 00:29:45
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.1.0/24 is directly connected, Ethernet0/0
L        172.16.1.1/32 is directly connected, Ethernet0/0
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, Serial2/0
L        192.168.1.1/32 is directly connected, Serial2/0
B     192.168.3.0/24 [200/0] via 172.16.1.2, 00:31:07
                     [RPR][200/0] via 192.168.1.2, 00:31:07
B     192.168.9.0/24 [20/0] via 192.168.1.2, 00:29:45
                     [RPR][20/0] via 192.168.3.2, 00:29:45
B     192.168.13.0/24 [20/0] via 192.168.1.2, 00:29:45
                      [RPR][20/0] via 192.168.3.2, 00:29:45

Device# show ip route repair-paths 10.9.9.9

>Routing entry for 10.9.9.9/32
>  Known via "bgp 100", distance 20, metric 0
>  Tag 10, type external
>  Last update from 192.168.1.2 00:44:52 ago
>  Routing Descriptor Blocks:
>  * 192.168.1.2, from 192.168.1.2, 00:44:52 ago, recursive-via-conn
>      Route metric is 0, traffic share count is 1
>      AS Hops 2
>      Route tag 10
>      MPLS label: none
>    [RPR]192.168.3.2, from 172.16.1.2, 00:44:52 ago
>      Route metric is 0, traffic share count is 1
>      AS Hops 2
>      Route tag 10
>      MPLS label: none
```

show ip route rip

To display contents of the RIP routing table, use the **show ip route rip** command in privileged EXEC mode.

show ip route rip | [append *resource-locator* **| begin** *LINE* **| count** *LINE* **| exclude** *LINE* **| format** *file-location* **| include** *LINE* **| redirect** *resource-locator* **| section** *LINE* **| tee** *resource-locator* **]**

Syntax Description

append	Appends redirected output to URL (URLs supporting append operation only).
begin	Begins with the line that matches.
count	Counts number of lines which match regexp.
exclude	Excludes lines that match.
format	Formats the output using the specified spec file.
include	Includes lines that match.

redirect	Redirects output to URL.
section	Filters a section of output.
tee	Copies output to URL.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

Example

The following sample output displays the IP routing table associated with RIP:

```
Device# show ip route rip
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected

Gateway of last resort is 10.0.5.13 to network 10.10.10.10

R     10.11.0.0/16 [120/1] via 172.16.1.2, 00:00:02, GigabitEthernet1
```

show ip route vrf

To display the IP routing table associated with a specific VPN routing and forwarding (VRF) instance, use the **show ip route vrf** command in user EXEC or privileged EXEC mode.

show ip route vrf { *vrf-name* | * } [**connected** | *protocol* [*as-number*] | **list** [*list-number*] | **profile** | **static** | **summary** | [*ip-prefix/ip-address*] [*mask* | **longer-prefixes**] | **repair-paths** | **dhcp** | **supernets-only** | **tag** { *tag-value* | *tag-value-dotted-decimal* [*mask*] }]

Syntax Description

*vrf-name or **	Name of the VRF. Use the asterisk (*) wildcard to include all the VRFs.
connected	(Optional) Displays all the connected routes in a VRF.

protocol	(Optional) Routing protocol. To specify a routing protocol, use one of these keywords: **bgp**, **egp**, **eigrp**, **hello**, **igrp**, **isis**, **ospf**, or **rip**.
as-number	(Optional) Autonomous system number.
list *number*	(Optional) Specifies the IP access list to be displayed.
profile	(Optional) Displays the IP routing table profile.
static	(Optional) Displays static routes.
summary	(Optional) Displays a summary of routes.
ip-prefix	(Optional) Network for which routing information is displayed.
ip-address	(Optional) Address for which routing information is displayed.
mask	(Optional) Network mask.
longer-prefixes	(Optional) Displays longer prefix entries.
repair-paths	(Optional) Displays repair paths.
dhcp	(Optional) Displays routes added by the DHCP server.
supernets-only	(Optional) Displays only supernet entries.
tag	(Optional) Displays information about route tags in the VRF table.
tag-value	(Optional) Route tag values as a plain decimals.
tag-value-dotted-decimal	(Optional) Route tag values as a dotted decimals.
mask	(Optional) Route tag wildcard mask.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This command was modified. Supports inter-service VPNs route leaking and redistribution.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE show ip route vrf command.

Examples

The following is a sample output from the **show ip route vrf** *vrf-name* command displaying routes under VRF 2 table:

```
Device# show ip route vrf 2
Routing Table: 2
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
S   +    10.10.10.97/32 [1/0] via 10.20.1.2 (1)
C        10.20.2.0/24 is directly connected, GigabitEthernet5
L        10.20.2.1/32 is directly connected, GigabitEthernet5
```

The following is a sample output from the **show ip route vrf** *vrf-name* **rip** command displaying RIP routes under a VRF table:

```
Device# show ip route vrf 1 rip
Routing Table: 1
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
H - NHRP, G - NHRP registered, g - NHRP registration summary
o - ODR, P - periodic downloaded static route, l - LISP
a - application route
+ - replicated route, % - next hop override, p - overrides from PfR
& - replicated local route overrides by connected

Gateway of last resort is not set

10.14.0.0/32 is subnetted, 1 subnets
R 10.14.14.14 [120/1] via 10.20.25.18, 00:00:18, GigabitEthernet5
```

The following is a sample output from the **show ip route vrf** command, displaying the IP routing table associated with a VRF named 1:

```
Device# show ip route vrf 1
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       I - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR
       T - traffic engineered route

Gateway of last resort is not set

B    10.0.0.0/8 [200/0] via 10.13.13.13, 00:24:19
C    10.0.0.0/8 is directly connected, GigabitEthernet1/3
B    10.0.0.0/8 [20/0] via 10.0.0.1, 02:10:22
B    10.0.0.0/8 [200/0] via 10.13.13.13, 00:24:20
```

This following is a sample output from the **show ip route vrf** *vrf-name* **rip** command using the **bgp** keyword, displaying BGP entries in the IP routing table associated with a VRF named 1:

```
Device# show ip route vrf 1 bgp
B  10.0.0.0/8 [200/0] via 10.13.13.13, 03:44:14
B  10.0.0.0/8 [20/0] via 10.0.0.1, 03:44:12
B  10.0.0.0/8 [200/0] via 10.13.13.13, 03:43:14
```

The following is a sample output from the **show ip route vrf** command, displaying repair paths in the routing table. The fields in the display are self-explanatory:

```
Device# show ip route vrf test1 repair-paths 192.168.3.0
Routing Table: test1
Routing entry for 192.168.3.0/24
  Known via "bgp 10", distance 20, metric 0
  Tag 100, type external
  Last update from 192.168.1.1 00:49:39 ago
  Routing Descriptor Blocks:
  * 192.168.1.1, from 192.168.1.1, 00:49:39 ago, recursive-via-conn
      Route metric is 0, traffic share count is 1
      AS Hops 1
      Route tag 100
      MPLS label: none
    [RPR]10.4.4.4 (default), from 10.5.5.5, 00:49:39 ago, recursive-via-host
      Route metric is 0, traffic share count is 1
      AS Hops 1
      Route tag 100
      MPLS label: 29
MPLS Flags: MPLS Required, No Global
```

Using wildcard for VRF name

This example uses the asterisk (*) wildcard for *vrf-name*, with the **summary** keyword. All the VRFs are included, in this case, **default**, **blue**, and **red**.

```
Device# show ip route vrf * summary
IP routing table name is default (0x0)
IP routing table maximum-paths is 32
Route Source    Networks    Subnets     Replicates  Overhead    Memory (bytes)
application     0           0           0           0           0
connected       0           2           0           192         624
static          1           1           0           192         624
internal        1                                               672
Total           2           3           0           384         1920

IP routing table name is blue (0x2)
IP routing table maximum-paths is 32
Route Source    Networks    Subnets     Replicates  Overhead    Memory (bytes)
application     0           0           0           0           0
connected       0           0           0           0           0
static          0           0           0           0           0
internal        0                                               40
Total           0           0           0           0           40

IP routing table name is red (0x5)
IP routing table maximum-paths is 32
Route Source    Networks    Subnets     Replicates  Overhead    Memory (bytes)
application     0           0           0           0           0
connected       0           0           0           0           0
```

```
static          0           0           0           0           0
internal        0                                               40
Total           0           0           0           0           40
```

show ip sla summary

To display summary statistics for IP Service Level Agreements (SLA) operations, use the **show ip sla summary** command in privileged EXEC mode.

show ip sla summary

destination	(Optional) Displays destination-address-based statistics.
destination-ip-address	IP address of the destination device.
destination-hostname	Hostname of the destination device.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.2(3)T	This command was introduced.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S.
15.1(2)SG	This command was integrated into Cisco IOS Release 15.1(2)SG.
Cisco IOS XE Release 3.4SG	This command was integrated into Cisco IOS XE Release 3.4SG.
15.3(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command is supported for Cisco Catalyst SD-WAN.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE show ip sla summary command.

Examples

The following is a sample output from the **show ip sla summary** command:

```
Device# show ip sla summary
IPSLAs Latest Operation Summary
Codes: * active, ^ inactive, ~ pending
All Stats are in milliseconds. Stats with u are in microseconds

ID     Type    Destination  Stats     Return      Last
                                      Code        Run
---------------------------------------------------------------------------------------------
```

```
*53    http     10.1.1.1     RTT=2      OK  35 seconds ago
*54    http     10.1.1.10    RTT=2      OK  1 minute, 35 seconds ago
```

The following table describes the significant fields shown in the display:

Table 96: show ip sla summary command Field Descriptions

Field	Description
ID	IP SLA operations identifier.
Destination	IP address or hostname of the destination device for the listed operation.
Stats	RTT, in milliseconds.

show ipv6 access-list

To display the contents of all current IPv6 access lists, use the **show ipv6 access-list** command in privileged EXEC mode.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	This command is supported in Cisco Catalyst SD-WAN

Usage Guidelines

For usage guidelines, see the Cisco IOS XE show ipv6 access-list command.

Example

The following example displays the contents of all current IPv6 access lists.

```
Device#show ipv6 access-list
IPv6 access list seq_1-seq-rule1-v6-acl_
    permit ipv6 object-group source_prefix object-group dest_prefix sequence 11
```

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

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For more information about this command, see the Cisco IOS XE show ipv6 dhcp binding command.

The following is sample output from the show ipv6 dhcp binding command displays all automatic client bindings from the DHCP for IPv6 server binding table.

DHCPv6 Address Allocation

```
Device# show ipv6 dhcp binding
Client: FE80::250:56FF:FEBD:8261
  DUID: 00030001001EE6DBF500
  Username : unassigned
  VRF : 10
  IA NA: IA ID 0x00080001, T1 10000, T2 16000
    Address: 5001:DB8:1234:42:500C:B3FA:54A7:F63D
             preferred lifetime 20000, valid lifetime 20000
             expires at Oct 26 2021 01:17 PM (19925 seconds)
```

DHCPv6 Prefix Delegation

```
Device# show ipv6 dhcp binding
Client: FE80::250:56FF:FEBD:8261
  DUID: 00030001001EE6DBF500
  Username : unassigned
  VRF : 10
  Interface : GigabitEthernet0/0/3
  IA PD: IA ID 0x00080001, T1 100, T2 160
    Prefix: 2001:BB8:1602::/48
             preferred lifetime 200, valid lifetime 200
             expires at Oct 26 2021 08:01 AM (173 seconds
```

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.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

The following is sample output from the show ipv6 dhcp database command.

The following is sample output from the show ipv6 dhcp pool command to DHCP for IPv6 configuration pool information.

```
Device# show ipv6 dhcp database
Database agent bootflash:
  write delay: 300 seconds, transfer timeout: 300 seconds
  last written at Oct 26 2021 08:01 AM, write timer expires in 250 seconds
  last read at never
  successful read times 0
  failed read times 0
  successful write times 2
  failed write times 0
```

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.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For more information about this command, see the Cisco IOS XE show ipv6 dhcp interface command

The following is sample output from the show ipv6 dhcp interface command to display DHCP for IPv6 interface information.

DHCPv6 Address Allocation

```
Device# show ipv6 dhcp interface GigabitEthernet0/0/2
GigabitEthernet0/0/2 is in client mode
  Prefix State is IDLE
  Address State is OPEN
  Renew for address will be sent in 00:01:09
  List of known servers:
    Reachable via address: FE80::250:56FF:FEBD:DBD1
    DUID: 00030001001EBD43F800
    Preference: 0
    Configuration parameters:
      IA NA: IA ID 0x00080001, T1 100, T2 160
        Address: 2010:AB8:0:1:95D1:CFC:F227:23FB/128
                 preferred lifetime 200, valid lifetime 200
                 expires at Oct 26 2021 07:28 AM (170 seconds)
      DNS server: 2001:DB8:3000:3000::42
      Domain name: example.com
      Information refresh time: 0
      Vendor-specific Information options:
          Enterprise-ID: 100
  Prefix Rapid-Commit: disabled
  Address Rapid-Commit: disabled
```

DHCPv6 Prefix Delegation

```
Device# show ipv6 dhcp interface GigabitEthernet0/0/2
GigabitEthernet0/0/2 is in client mode
  Prefix State is OPEN
  Renew will be sent in 00:01:34
  Address State is IDLE
  List of known servers:
    Reachable via address: FE80::250:56FF:FEBD:DBD1
    DUID: 00030001001EBD43F800
    Preference: 0
    Configuration parameters:
      IA PD: IA ID 0x00080001, T1 100, T2 160
        Prefix: 2001:DB8:1202::/48
                 preferred lifetime 200, valid lifetime 200
                 expires at Oct 26 2021 07:30 AM (194 seconds)
      DNS server: 2001:DB8:3000:3000::42
      Domain name: example.com
      Information refresh time: 0
  Prefix name: prefix_from_server
```

```
  Prefix Rapid-Commit: disabled
  Address Rapid-Commit: disabled
```

DHCPv6 with SLAAC

```
Device# show ipv6 dhcp interface GigabitEthernet0/0/2
GigabitEthernet0/0/2 is in client mode
  Prefix State is IDLE (0)
  Information refresh timer expires in 23:59:49
  Address State is IDLE
  List of known servers:
    Reachable via address: FE80::250:56FF:FEBD:DBD1
    DUID: 00030001001EBD43F800
    Preference: 0
    Configuration parameters:
      DNS server: 2001:DB8:3000:3000::42
      Domain name: example.com
      Information refresh time: 0
      Vendor-specific Information options:
          Enterprise-ID: 100
  Prefix Rapid-Commit: disabled
  Address Rapid-Commit: disabled
```

show ipv6 dhcp pool

To display Dynamic Host Configuration Protocol (DHCP) for IPv6 configuration pool information, use the **show ipv6 dhcp pool** command in user EXEC or privileged EXEC mode.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For more information about this command, see the Cisco IOS XE show ipv6 dhcp pool command.

The following is sample output from the show ipv6 dhcp pool command to DHCP for IPv6 configuration pool information.

DHCPv6 Address Allocation

```
Device# show ipv6 dhcp pool
DHCPv6 pool: relay_server
  VRF 10
  Prefix pool: dhcpv6-pool2
  Address allocation prefix: 5001:DB8:1234:42::/64 valid 20000 preferred 20000 (1 in use,
0 conflicts)
               preferred lifetime 200, valid lifetime 200
  DNS server: 2001:BB8:3000:3000::42
  Domain name: relay.com
  Information refresh: 60
  Vendor-specific Information options:
  Enterprise-ID: 10
    suboption 1 address 2001:DB8:1234:42::10
    suboption 2 ascii 'ip phone'
  Active clients: 1
  Pool is configured to include all configuration options in REPLY
```

DHCPv6 Prefix Delegation

```
Device# show ipv6 dhcp pool
DHCPv6 pool: relay_server
  VRF 10
  Prefix pool: dhcpv6-pool2
  Address allocation prefix: 5001:DB8:1234:42::/64 valid 20000 preferred 20000 (0 in use,
0 conflicts)
               preferred lifetime 200, valid lifetime 200
  DNS server: 2001:BB8:3000:3000::42
  Domain name: relay.com
  Information refresh: 60
  Vendor-specific Information options:
  Enterprise-ID: 10
    suboption 1 address 2001:DB8:1234:42::10
    suboption 2 ascii 'ip phone'
  Active clients: 1
  Pool is configured to include all configuration options in REPLY
```

show ipv6 route vrf

To display IPv6 routing table information that is associated with a VPN routing and forwarding (VRF) instance, use the **show ipv6 route vrf** command in privileged EXEC mode.

show ipv6 route vrf *table name/vrf-id*

Syntax Description

table name/vrf-id	Table name or VRF identifier.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE show ipv6 route vrf command.

The following is a sample output from the **show ipv6 route vrf** command displaying information about the IPv6 routing table that is associated with VRF 1:

```
Device# show ipv6 route vrf 1
IPv6 Routing Table - 1 - 11 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, RL - RPL, O - OSPF Intra, OI - OSPF Inter
       OE1 - OSPF ext 1, OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1
       ON2 - OSPF NSSA ext 2, la - LISP alt, lr - LISP site-registrations
       ld - LISP dyn-eid, lA - LISP away, le - LISP extranet-policy
       lp - LISP publications, ls - LISP destinations-summary, a - Application
       m - OMP
R   1100::/64 [120/2]
     via FE80::20C:29FF:FE2E:13FF, GigabitEthernet2
R   2000::/64 [120/2]
     via FE80::20C:29FF:FE51:762F, GigabitEthernet2
R   2001:10::/64 [120/2]
     via FE80::20C:29FF:FE82:D659, GigabitEthernet2
```

```
R   2500::/64 [252/11], tag 44270
     via FE80::20C:29FF:FEE1:5237, GigabitEthernet2
C   2750::/64 [0/0]
     via GigabitEthernet2, directly connected
L   2750::1/128 [0/0]
     via GigabitEthernet2, receive
R   2777::/64 [252/11], tag 44270
     via FE80::20C:29FF:FEE1:5237, GigabitEthernet2
m   2900::/64 [251/0]
     via 192.168.1.5%default
R   3000::/64 [120/2]
     via FE80::20C:29FF:FE2E:13FF, GigabitEthernet2
R   3400::/64 [252/11], tag 44270
     via FE80::20C:29FF:FE51:762F, GigabitEthernet2
L   FF00::/8 [0/0]
     via Null0, receive
```

show key chain

To display authentication key information, use the **showkeychain** command in EXEC mode.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	This command was introduced.

Usage Guidelines

For more information about this command, see the Cisco IOS XE show key chain

Examples

The following is sample output from the **showkeychain** command:

```
Device# show key chain
Key-chain trees:
    key 1 -- text "chestnut"
        accept lifetime (always valid) - (always valid) [valid now]
        send lifetime (always valid) - (always valid) [valid now]
    key 2 -- text "birch"
        accept lifetime (00:00:00 Dec 5 2020) - (23:59:59 Dec 5 2020)
        send lifetime (06:00:00 Dec 5 2020) - (18:00:00 Dec 5 2020)
```

show lacp

To display Link Aggregation Control Protocol (LACP) channel-group information, use the **show lacp** command in privileged EXEC mode.

show lacp [*channel-group-number* | { **counters** | **internal** | **neighbor** | **sys-id** }]

Syntax Description

channel-group-number	(Optional) Channel group number. The range is 1 to 128.
counters	Displays traffic information.
internal	Displays internal information.

neighbor	Displays neighbor information.
sys-id	Displays the system identifier that is being used by LACP. The system identifier consists of the LACP system priority and the device MAC address.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	This command was introduced.

Usage Guidelines

You can enter any **show lacp** command to display the active channel-group information. To display specific channel information, enter the **show lacp** command with a channel-group number.

If you do not specify a channel group, information for all channel groups appears.

You can enter the channel-group-number to specify a channel group for all keywords except **sys-id**

Examples

The following is a sample output from the **show lacp counters** privileged EXEC command.

```
Device# show lacp counters
LACPDUs Marker Marker Response LACPDUs
Port Sent Recv Sent Recv Sent Recv Pkts Err
---------------------------------------------------------------------
Channel group: 10
Te0/1/0 51 0 0 0 0 0 0
Te0/1/1 60 52 0 0 0 0 0
```

Examples

The following is a sample output from the **show lacp internal** privileged EXEC command.

```
Device# show lacp internal
Flags: S - Device is requesting Slow LACPDUs
F - Device is requesting Fast LACPDUs
A - Device is in Active mode P - Device is in Passive mode

Channel group 10
LACP port Admin Oper Port Port
Port Flags State Priority Key Key Number State
Te0/1/0 SA susp 32768 0xA 0xA 0x41 0x7D
Te0/1/1 SA bndl 32768 0xA 0xA 0x42 0x3D
```

Examples

The following is a sample output from the **show lacp neighbor** privileged EXEC command.

```
Device# show lacp neighbor
Flags: S - Device is requesting Slow LACPDUs
F - Device is requesting Fast LACPDUs
A - Device is in Active mode P - Device is in Passive mode
```

```
Channel group 10 neighbors

LACP port Admin Oper Port Port
Port Flags Priority Dev ID Age key Key Number State
Te0/1/0 SP 0 0000.0000.0000 420125s 0x0 0x0 0x0 0x0
Te0/1/1 SP 32768 3c13.cc93.4100 26s 0x0 0x1 0x4 0x3C
```

Examples

The following is a sample output from the **show lacp sys-id** privileged EXEC command.

```
Device# show lacp sys-id
32765,0002.4b29.3a00
```

show lte450 all

To display comprehensive information about all LTE450 module, use the **show lte450** command in privileged EXEC (#) mode.

show lte450 *slot_number* **all**

Syntax Description

all	Shows all the details of the P-LTE-450 module.
slot_number	Slot number where the P-LTE-450 module is installed.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.18.1a	This command is supported in Cisco Catalyst SD-WAN.

Examples

The following sample output displays the network details, including including hardware, radio, and network status.

```
Device# show lte450 0/1/0 all
System Status
=============
System time = Wed May 21 05:31:44 2025
Uptime = 2h 34m 24s
Load Average = 2.47 2.53 2.54
Free Disk space = 89204 KB
Free RAM = 54944 KB

Modem information
=================
Modem MAC = 88:5D:90:EF:FF:FF
Modem hardware version = ML620EU
Modem firmware version = 0.3.4.1/ML620EUV13_RELEASE_20240305
Modem temperature = 48.0 deg C
```

```
PIM information
===============
PIM MAC = FC:C2:3D:30:E3:F2
PIM hardware version = IPS-701-V3
PIM firmware version = IPS701-v1.3.0-Secured
PIM serial number = 50030301564
Management IPv4 Address = 192.168.200.1
Management IPv6 Address = fd00:ffff:c0:a8c8::1/64
PIM temperature = 50.0 deg C

GNSS Location Data
==================
Latitude =
Longitude =
Altitude =
Time =

Watchdog Statistics
===================
Hardware watchdog counter = 0
Modem watchdog counter = 0

Mobile network status
=====================
Connection Status = Online
Connection time = 2h 31m 54s
IMSI = 001010123456058
ICCID = 89860001010123456789
MSISDN =
APN-1 IPv4 address = 192.168.4.38
APN-1 IPv6 address = 2001:0468:3000:0008:2001:0468:3000:0008
APN-2 IPv4 address =
APN-2 IPv6 address =
APN-3 IPv4 address =
APN-3 IPv6 address =

Mobile connection information
=============================
IMEI = 862128050313077
System mode = LTE
EPS State = ATTACHED
RRC State = RRC IDLE
CEREG = 1
APN-1 APN name = ims.mnc001.mcc001.gprs
APN-2 APN name =
APN-3 APN name =
Band = 31
PLMN = 00101
Cell ID = 27447298
TAC = 0(1)
PCI = 2
TX power = 0
Bandwidth = 5MHz
LTE RX channel = 9895
LTE TX channel = 27785
Current upload = 0.0 Kbps
Current download = 0.0 Kbps

Signal quality
==============
RSSI = -77 dBm
RSRP = -99 dBm
RSRQ = -8 dB
SINR = 5 dB
```

```
Antenna signal quality
======================
Main RSSI = -78 dBm
Main RSRP = -101 dBm
Aux RSSI = -77 dB
Aux RSRP = -99 dB
```

show lte450 network

To display the network information about the P-LTE-450 module, use the **show lte450** command in privileged EXEC (#) mode.

show lte450 *slot_number* **network**

Syntax Description

network	Shows the network details.
slot_number	Slot number where the P-LTE-450 module is installed.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.18.1a	This command is supported in Cisco Catalyst SD-WAN.

Examples

The following sample output displays the network details, including network status, and connection information.

```
Device# show lte450 0/1/0 network

Mobile network status
=====================
Connection Status = Online
Connection time = 2h 31m 21s
IMSI = 001010123456058
ICCID = 89860001010123456789
MSISDN =
APN-1 IPv4 address = 192.168.4.38
APN-1 IPv6 address = 2001:0468:3000:0008:2001:0468:3000:0008
APN-2 IPv4 address =
APN-2 IPv6 address =
APN-3 IPv4 address =
APN-3 IPv6 address =

Mobile connection information
=============================
IMEI = 862128050313077
System mode = LTE
EPS State = ATTACHED
RRC State = RRC IDLE
CEREG = 1
APN-1 APN name = ims.mnc001.mcc001.gprs
```

```
APN-2 APN name =
APN-3 APN name =
Band = 31
PLMN = 00101
Cell ID = 27447298
TAC = 0(1)
PCI = 2
TX power = 0
Bandwidth = 5MHz
LTE RX channel = 9895
LTE TX channel = 27785
Current upload = 0.0 Kbps
Current download = 0.0 Kbps
```

show lte450 hardware

To display the hardware-related information about the P-LTE-450 module, use the **show lte450** command in privileged EXEC (#) mode.

show lte450 *slot_number* **hardware**

Syntax Description

hardware	Shows the hardware details.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.18.1a	This command is supported in Cisco Catalyst SD-WAN.

Examples

The following sample output displays the hardware details, including modem and PIM details, GNSS, and watchdog statistics.

```
Device# show lte450 0/1/0 hardware
 System Status
=============
System time = Wed May 21 05:31:08 2025
Uptime = 2h 33m 48s
Load Average = 2.67 2.56 2.55
Free Disk space = 89204 KB
Free RAM = 54944 KB

Modem information
=================
Modem MAC = 88:5D:90:EF:FF:FF
Modem hardware version = ML620EU
Modem firmware version = 0.3.4.1/ML620EUV13_RELEASE_20240305
Modem temperature = 48.0 deg C

PIM information
===============
PIM MAC = FC:C2:3D:30:E3:F2
```

```
PIM hardware version = IPS-701-V3
PIM firmware version = IPS701-v1.3.0-Secured
PIM serial number = 50030301564
Management IPv4 Address = 192.168.200.1
Management IPv6 Address = fd00:ffff:c0:a8c8::1/64
PIM temperature = 49.5 deg C

GNSS Location Data
==================
Latitude =
Longitude =
Altitude =
Time =

Watchdog Statistics
===================
Hardware watchdog counter = 0
Modem watchdog counter = 0
```

show lte450 radio

To display the radio information about the P-LTE-450 module, use the **show lte450** command in privileged EXEC (#) mode.

show lte450 *slot_number* **radio**

Syntax Description

radio	Shows the radio details.
slot_number	Slot number where the P-LTE-450 module is installed.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.18.1a	This command is supported in Cisco Catalyst SD-WAN.

Examples

The following sample output displays the radio details, including signal quality and Antenna signal quality.

```
Device# show lte450 0/1/0 radio
Signal quality
==============
RSSI = -77 dBm
RSRP = -99 dBm
RSRQ = -8 dB
SINR = 5 dB

Antenna signal quality
======================
Main RSSI = -78 dBm
Main RSRP = -101 dBm
```

```
Aux RSSI = -77 dB
Aux RSRP = -99 dB
```

show logging cacert

To view the list of all installed certificates on the device along their date of expiry, use the **show logging cacert** command in privileged EXEC mode.

show logging cacert

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.13.1a	This command is supported for Cisco Catalyst SD-WAN.

Examples

The following is a sample output from the **show logging cacert** command that is used to display the list of all installed certificates on the device along their date of expiry. The fields shown in the display are self-explanatory.

```
Device# show logging cacert
INDEX  NAME      VALIDITY
-----------------------------------------
0      cert.pem  Fri Jun 21 20:35:10 2024
```

show logging profile sdwan internal filter

To view messages logged by binary trace for Cisco-SD-WAN-specific processes and process modules, use the **show logging profile sdwan internal filter** command in the privileged EXEC mode. The messages are displayed in chronological order.

show logging profile sdwan internal filter [*filter-string*]

Syntax Description

filter-string	Displays the filter for a specific SD-WAN instance. Range:1 to 65531

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.15.1a	This command was introduced.

Usage Guidelines

Use **show platform hardware qfp active feature bfd datapath sdwan summary** to get the local descriptor value for a session.

Examples

The following sample displays the show output from a logging profile for a device 20008:

```
Device# show logging profile sdwan internal filter string 20008

Logging display requested on 2024/06/18 09:12:56 (UTC) for Hostname: [cedge3], Model:
[C8000V], Version: [17.15.01], SN: [91KQWKQZRMD], MD_SN: [SSI130300YK]

Displaying logs from the last 0 days, 0 hours, 10 minutes, 0 seconds
executing cmd on chassis local ...
Unified Decoder Library Init .. DONE
Found 1 UTF Streams

2024/06/18 09:12:53.690092174 {ftmd_R0-0}{255}: [ftmd-bfd] [24539]: (debug): [LOGID:3] RA
enabled for LD value:20008
2024/06/18 09:12:53.691445109 {ftmd_R0-0}{255}: [ftmd-bfd] [24539]: (debug): [LOGID:11] BFD
 msg for ld(20008) with state (1) update reason (2)
2024/06/18 09:12:53.691505178 {ftmd_R0-0}{255}: [ftmd-bfd] [24539]: (debug): [LOGID:192]
tunnel_public_tloc_msg : ld 20008 tun_rec_index 8 tloc_index 32779 public tloc 0.0.0.0/0
2024/06/18 09:12:53.691549078 {ftmd_R0-0}{255}: [ftmd-bfd] [24539]: (debug): [LOGID:195]
tunnel_public_tloc_msg :  ld 20008 tloc_index 32779 already knows public tloc 0.0.0.0/0
2024/06/18 09:12:53.691550747 {ftmd_R0-0}{255}: [ftmd-ttm] [24539]: (debug): [LOGID:30] BFD
 session gone down
2024/06/18 09:12:53.691562033 {ftmd_R0-0}{255}: [ftmd-bfd] [24539]: (debug): [LOGID:175]
BFD-session TNL 172.16.13.254:12346->192.168.4.37:12346, : Increment the WAN interface
counters by 1
2024/06/18 09:12:53.691584809 {ftmd_R0-0}{255}: [ftmd-umts] [24539]: (debug): [LOGID:64]
free ctxt for probe PERIODIC lc biz-internet period 1800 src 172.16.13.254 dst 192.168.4.37
2024/06/18 09:12:53.691606267 {ftmd_R0-0}{255}: [ftmd-bfd] [24539]: (debug): [LOGID:39]
Sending Link BFD status message to TTM, status DOWN tun_idx 8,
172.16.255.13/biz-internet:172.16.255.17/mpls/IPSEC
2024/06/18 09:12:53.691614231 {ftmd_R0-0}{255}: [vipcommon-msgq] [24539]: (debug): Queued
Message of size 51 to target TTMD
2024/06/18 09:12:53.691698393 {ftmd_R0-0}{255}: [vipcommon-msgq] [24539]: (debug): Sent
Message of size 51 to target TTMD
2024/06/18 09:12:53.692575643 {ftmd_R0-0}{255}: [libjournal] [24539]: (debug): Write-Line
of msg:ttm to  Succeed
2024/06/18 09:12:53.692584386 {ftmd_R0-0}{255}: [ftmd-ttm] [24539]: (debug): [LOGID:77]
Received TLOC add from Caller:[tloc_replay_specific_tloc] , tloc Index: 32779 (tloc ID:
tloc_origin=REMOTE, tloc_id: 172.16.255.17 : mpls : ipsec) Origin REMOTE. Capability 0x3f.
 TLOC attribute: 0X1008012E0FE43A6
2024/06/18 09:12:53.692591033 {ftmd_R0-0}{255}: [ftmd-ttm] [24539]: (debug): [LOGID:38]
System 172.16.255.17, site 17, local 0, on_demand old 1, new 1
2024/06/18 09:12:53.692600925 {ftmd_R0-0}{255}: [ftmd-ttm] [24539]: (debug): [LOGID:100]
tloc_add  (REMOTE_TLOC)
2024/06/18 09:12:53.692606364 {ftmd_R0-0}{255}: [ftmd-ttm] [24539]: (debug): [LOGID:110]
tloc_index 32771 BFD Address Family is IPV4
2024/06/18 09:12:53.692608238 {ftmd_R0-0}{255}: [ftmd-ttm] [24539]: (debug): [LOGID:53] Not
 MRF Migration in Process, local tloc color: 2, remote tloc color 2, local tloc region id:
 0, remote tloc region id: 65534, remote site id: 17
2024/06/18 09:12:53.692610564 {ftmd_R0-0}{255}: [ftmd-ttm] [24539]: (debug): [LOGID:59]
Local site on_demand: True, Remote site 17, on_demand: False, Active
2024/06/18 09:12:53.692617126 {ftmd_R0-0}{255}: [ftmd-bfd] [24539]: (debug): [LOGID:42]
ftm-binos_bfd_sess_add : ENTER
2024/06/18 09:12:53.692622639 {ftmd_R0-0}{255}: [ftmd-bfd] [24539]: (debug): [LOGID:41] FTM
 create BFD internal pak - dst pvt: 192.168.4.37:12346
2024/06/18 09:12:53.692623822 {ftmd_R0-0}{255}: [ftmd-bfd] [24539]: (debug): [LOGID:46]
ftm-binos_bfd_sess_add : init symnat with  ZEROs
2024/06/18 09:12:53.692626824 {ftmd_R0-0}{255}: [ftmd-bfd] [24539]: (debug): [LOGID:47] BFD
 TLV attributes: Encap: 1, My_pub_ip:192.168.4.33, My_pub_port:12346, Remote_ip: 192.168.4.37,
```

```
 Remote_port: 12346, Max tunnel MTU: 0, capabilities: 0, Ipsec Overhead: 38
2024/06/18 09:12:53.692628621 {ftmd_R0-0}{255}: [ftmd-bfd] [24539]: (debug): [LOGID:48] Got
 session record color:2, local_color:2
2024/06/18 09:12:53.692630040 {ftmd_R0-0}{255}: [ftmd-bfd] [24539]: (debug): [LOGID:50] BFD
 Add Message FTM->FMAN-RP parameters Hello interval: 1000, Local Discriminator: 20007, Local
 color: 2, if_number: 7, session_type:IPV4, detect multiplier:7 max_tunnel_mtu:1442 BFD
State: UP, adj_id: 0xf810006f, capabilities: 352, ipsec_overhead: 38, poll interval: 600000,
 sdwan_bfd_flags: 0x1 my_pub_ip/port:192.168.4.33/12346 my_symnat_pub_ip/port:0.0.0.0/0
remote_ip/port:192.168.4.37/12346
2024/06/18 09:12:53.692654059 {ftmd_R0-0}{255}: [libjournal] [24539]: (debug): Write-Line
of msg:fman-rp to  Succeed
2024/06/18 09:12:53.694167194 {ftmd_R0-0}{255}: [ftmd-binos] [24539]: (debug): [LOGID:4]
send BINOS protobuf message(size=181)
2024/06/18 09:12:53.694169543 {ftmd_R0-0}{255}: [ftmd-bfd] [24539]: (debug): [LOGID:51]
ftm-binos_bfd_sess_add : EXIT
2024/06/18 09:12:53.694173216 {ftmd_R0-0}{255}: [ftmd-ttm] [24539]: (debug): [LOGID:118]
BFD session created for TLOC:32779:32771 is_up=UP is_suspended=No,  p_session:0x7627d2b9d960
2024/06/18 09:12:53.694177030 {ftmd_R0-0}{255}: [ftmd-ttm] [24539]: (debug): [LOGID:120]
attr_flag 31 downstream min 0,default 0 max 0, period 0 up 0
2024/06/18 09:12:53.694179927 {ftmd_R0-0}{255}: [ftmd-ttm] [24539]: (debug): [LOGID:110]
tloc_index 32770 BFD Address Family is IPV4
```

show macsec hw detail

To display detailed hardware-related information about MACsec on a Cisco IOS XE Catalyst SD-WAN device, use the **show macsec hw detail** command in privileged EXEC mode.

show macsec hw detail

Syntax Description

This command has no keywords or arguments.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	This command is supported for Cisco Catalyst SD-WAN.

Examples

This is sample output of the **show macsec hw detail** command.

```
Device# show macsec hw detail
MACsec Capable Interface         RxSA Inuse
-----------------------------------------------
 TenGigabitEthernet0/0/5       :        1


Other Debug Statistics
Interface TenGigabitEthernet0/0/5 HMAC:
RxOctets              0  RxUcastPkts           0  RxMcastPkts           0
RxBcastPkts           0  RxDiscards            0  RxErrors              0
TxOctets              0  TxUcastPkts           0  TxMcastPkts           0
TxBcastPkts           0  TxErrors              0
LMAC:
RxOctets           5595  RxUcastPkts          22  RxMcastPkts           9
RxBcastPkts           0  RxDiscards            0  RxErrors              0
TxOctets           1710  TxUcastPkts          15  TxMcastPkts           0
TxBcastPkts           0  TxErrors              0
```

show macsec mka-request-notify

To view information about MACsec (Media Access Control Security) enabled interfaces, including the counts of control plane transmit and delete secure channels, transmit security associations, receive secure channels, and delete security associations, as well as the MKA (MACsec Key Agreement) notification count on the interface **TenGigabitEthernet0/0/5**, use the **show macsec mka-request-notify** command in privileged EXEC mode.

show macsec mka-request-notify

Syntax Description

This command has no keywords or arguments.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	This command is supported for Cisco Catalyst SD-WAN.

Examples

This is sample output of the **show macsec mka-request-notify** command.

```
Device# show macsec mka-request-notify
MACsec Enabled Interface         CR_TX_SC  DEL_TX_SC  INST_TX_SA  CR_RX_SC  DEL_RX_SC
INST_RX_SA  DEL_RX_SA  MKA_NOTIFY
-------------------------------------------------------------------------------------
 TenGigabitEthernet0/0/5       :       18        17        18        18         0
18           11         0
```

show macsec summary

To display a summary of MACsec information on the device, including MACsec capable interfaces, installed secure channels, and MACsec enabled interfaces with their associated receive secure channels and VLAN, use the **show macsec summary** command in privileged EXEC mode.

show macsec summary

Syntax Description

This command has no keywords or arguments.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	This command is supported for Cisco Catalyst SD-WAN.

Examples

This is sample output of the **show macsec summary** command.

```
Device# show macsec summary
MACsec Capable Interface               Extension              Installed Rx SC
-------------------------------------------------------------------------------
 TenGigabitEthernet0/0/0                One tag-in-clear
```

```
 TenGigabitEthernet0/0/1                One tag-in-clear
 TenGigabitEthernet0/0/2                One tag-in-clear
 TenGigabitEthernet0/0/3                One tag-in-clear
 TenGigabitEthernet0/0/4                One tag-in-clear
 TenGigabitEthernet0/0/5                One tag-in-clear                 1
 TenGigabitEthernet0/0/6                One tag-in-clear
 TenGigabitEthernet0/0/7                One tag-in-clear
 TenGigabitEthernet0/1/0                One tag-in-clear
 TenGigabitEthernet0/1/1                One tag-in-clear
 TenGigabitEthernet0/1/2                One tag-in-clear
 TenGigabitEthernet0/1/3                One tag-in-clear
 FortyGigabitEthernet0/2/0              One tag-in-clear
 FortyGigabitEthernet0/2/4              One tag-in-clear
 FortyGigabitEthernet0/2/8              One tag-in-clear
 GigabitEthernet0                       One tag-in-clear
 SDWAN System Intf IDB                  One tag-in-clear
 SDWAN vmanage_system IDB               One tag-in-clear
 LIIN0                                  One tag-in-clear
 LI-Null0                               One tag-in-clear
 Loopback65528                          One tag-in-clear
 Loopback65529                          One tag-in-clear
 SR0                                    One tag-in-clear
 Tunnel1                                One tag-in-clear
 VoIP-Null0                             One tag-in-clear

 MACsec Enabled Interface         Receive SC   VLAN
-----------------------------------------------------
 TenGigabitEthernet0/0/5       :        1         0
```

show macsec status interface

To display the MACsec configuration and status of an interface, use the **show macsec status interface** command in privileged EXEC mode.

show macsec status interface

Syntax Description

This command has no keywords or arguments.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	This command is supported for Cisco Catalyst SD-WAN.

Examples

This is sample output of the **show macsec status interface** command.

```
Device# show macsec status interface TenGigabitEthernet 0/0/5
Capabilities:
  Ciphers Supported:        GCM-AES-128 GCM-AES-256 GCM-AES-XPN-128 GCM-AES-XPN-256
  Cipher:                   GCM-AES-128
  Confidentiality Offset:   0
  Replay Window:            64
  Delay Protect Enable:     FALSE
  Access Control:           must-secure
  Include-SCI:              TRUE

 Transmit SC:
```

```
 SCI:                      E8D322D32085000D
 Transmitting:             TRUE
Transmit SA:
 Next PN:                  10002
 Delay Protect AN/nextPN:  NA/0

Receive SC:
 SCI:                      A03D6E5D037F0045
 Receiving:                TRUE
Receive SA:
 Next PN:                  10077
 AN:                       1
 Delay Protect AN/LPN:     0/0
```

show mka default-policy

To display information about the MACsec Key Agreement (MKA) Protocol default policy, use the **show mka default-policy** command in privileged EXEC mode.

show mka default-policy [{ **sessions detail** } | **session detail**]

Syntax Description

sessions	(Optional) Displays a summary of active MKA sessions that have the default policy applied.
Detail	(Optional) Displays detailed configuration information for the default policy and the interface names to which the default policy is applied, or displays detailed status information about all active MKA sessions that have the default policy applied.

Syntax Description

This command has no keywords or arguments.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	This command is supported for Cisco Catalyst SD-WAN.

Examples

This is sample output of the **show mka default-policy detail** command:

```
Device# show mka default-policy detail
MKA Policy Configuration ("*DEFAULT POLICY*")
=========================
MKA Policy Name...........*DEFAULT POLICY*
Key Server Priority.......0
Confidentiality Offset....0
Delay Protect.............FALSE
SAK-Rekey On-Peer-Loss....0
SAK-Rekey Interval........0
Send Secure Announcement..DISABLED
Include ICV Indicator.....TRUE
SCI Based SSCI............FALSE
Use Updated Ethernet Hdr..NO
Cipher Suite(s)........ GCM-AES-128
                        GCM-AES-256

Applied Interfaces...
```

Examples

The following is a sample output from the **show mka default-policy sessions** command.

```
Device# show mka default-policy sessions
Summary of All Active MKA Sessions with MKA Policy "*DEFAULT POLICY*"...

=============================================================================================
Interface       Local-TxSCI          Policy-Name       Inherited          Key-Server

Port-ID         Peer-RxSCI           MACsec-Peers      Status             CKN

=============================================================================================
Te0/0/5         e8d3.22d3.2085/000d  *DEFAULT POLICY*  NO                 NO

13              a03d.6e5d.037f/0045  1                 Secured            10
```

The following is a sample output from the **show mka default-policy sessions detail** command.

```
Device# show mka default-policy sessions detail

MKA Detailed Status for MKA Session
===================================
Status: SECURED - Secured MKA Session with MACsec

Local Tx-SCI..... e8d3.22d3.2085/000d
Interface MAC Address.... e8d3.22d3.2085
MKA Port Identifier..... 13
Interface Name..... TenGigabitEthernet0/0/5
Audit Session ID.....
CAK Name (CKN)..... 10
Member Identifier (MI)... DE832E171DCC70441E997F96
Message Number (MN)..... 80
EAP Role..... NA
Key Server..... NO
MKA Cipher Suite..... AES-256-CMAC

Latest SAK Status..... Rx & Tx
Latest SAK AN..... 1
Latest SAK KI (KN)..... 811368FD2F9F9CC82C1894C800000012 (18)
Old SAK Status..... No Rx, No Tx
Old SAK AN..... 0
Old SAK KI (KN)..... RETIRED (0)

SAK Transmit Wait Time... 0s (Not waiting for any peers to respond)
SAK Retire Time..... 0s (No Old SAK to retire)
SAK Rekey Time..... 0s (SAK Rekey interval not applicable)

MKA Policy Name..... *DEFAULT POLICY*
Key Server Priority..... 0
Delay Protection..... NO
Delay Protection Timer..... 0s (Not enabled)

Confidentiality Offset... 0
Algorithm Agility..... 80C201
SAK Rekey On Live Peer Loss..... NO
Send Secure Announcement.. DISABLED
SCI Based SSCI Computation.... NO
SAK Cipher Suite..... 0080C20001000001 (GCM-AES-128)
MACsec Capability..... 3 (MACsec Integrity, Confidentiality, & Offset)
MACsec Desired..... YES

# of MACsec Capable Live Peers..... 1
# of MACsec Capable Live Peers Responded.. 0
```

```
Live Peers List:
  MI                        MN          Rx-SCI (Peer)        KS        RxSA          SSCI
                                                             Priority  Installed
  ------------------------------------------------------------------------------------------
  811368FD2F9F9CC82C1894C8  379101      a03d.6e5d.037f/0045  0         YES            0

Potential Peers List:
  MI                        MN          Rx-SCI (Peer)        KS        RxSA          SSCI
                                                             Priority  Installed
  ------------------------------------------------------------------------------------------

Dormant Peers List:
  MI                        MN          Rx-SCI (Peer)        KS        RxSA          SSCI
                                                             Priority  Installed
  ------------------------------------------------------------------------------------------


MKA Detailed Status for MKA Session
===================================
Status: INITIALIZING - Searching for Peer (Waiting to receive first Peer MKPDU)

Local Tx-SCI.............. e8d3.22d3.2085/000d
Interface MAC Address.... e8d3.22d3.2085
MKA Port Identifier...... 13
Interface Name........... TenGigabitEthernet0/0/5
Audit Session ID.........
CAK Name (CKN)........... 11
Member Identifier (MI)... 6758F1CA5F050202DC742B03
Message Number (MN)...... 79
EAP Role................. NA
Key Server............... YES
MKA Cipher Suite......... AES-256-CMAC

Latest SAK Status........ Rx & Tx
Latest SAK AN............ 1
Latest SAK KI (KN)....... 811368FD2F9F9CC82C1894C800000012 (18)
Old SAK Status........... No Rx, No Tx
Old SAK AN............... 0
Old SAK KI (KN).......... RETIRED (0)

SAK Transmit Wait Time... 0s (Not waiting for any peers to respond)
SAK Retire Time.......... 0s (No Old SAK to retire)
SAK Rekey Time........... 0s (SAK Rekey interval not applicable)

MKA Policy Name.......... *DEFAULT POLICY*
Key Server Priority...... 0
Delay Protection......... NO
Delay Protection Timer.......... 0s (Not enabled)

Confidentiality Offset... 0
Algorithm Agility........ 80C201
SAK Rekey On Live Peer Loss........ NO
Send Secure Announcement.. DISABLED
SCI Based SSCI Computation.... NO
SAK Cipher Suite......... 0080C20001000001 (GCM-AES-128)
MACsec Capability........ 3 (MACsec Integrity, Confidentiality, & Offset)
MACsec Desired........... YES

# of MACsec Capable Live Peers............ 0
# of MACsec Capable Live Peers Responded.. 0

Live Peers List:
  MI                        MN          Rx-SCI (Peer)        KS        RxSA          SSCI
                                                             Priority  Installed
```

```
  ------------------------------------------------------------------------------------

Potential Peers List:
  MI                      MN          Rx-SCI (Peer)        KS        RxSA          SSCI
                                                           Priority  Installed
  ------------------------------------------------------------------------------------

Dormant Peers List:
  MI                      MN          Rx-SCI (Peer)        KS        RxSA          SSCI
                                                           Priority  Installed
  ------------------------------------------------------------------------------------
```

show mka keychains

To display the list of MACsec keychains configured on a Cisco IOS XE Catalyst SD-WAN device, use the **show mka keychains** command in privileged EXEC mode.

show mka keychains

Syntax Description

This command has no keywords or arguments.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	This command is supported for Cisco Catalyst SD-WAN.

Examples

This is sample output of the **show mka keychains** command.

```
Device# show mka keychains

MKA PSK Keychain(s) Summary...

Keychain         Latest CKN                                                    Interface(s)
Name              Latest CAK                                                       Applied

=============================================================================================
mka-keychain128  10                                                             Te0/0/5

                 <HIDDEN>
```

show mka policy

To display the MACsec policies configured on a Cisco IOS XE Catalyst SD-WAN device, use the **show mka default-policy** command in privileged EXEC mode.

show mka default-policy

Syntax Description

This command has no keywords or arguments.

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	This command is supported for Cisco Catalyst SD-WAN.

Examples

This is sample output of the **show mka default-policy** command:

```
Device# show mka policy MKA-128
MKA Policy Summary...

Codes : CO - Confidentiality Offset, ICVIND - Include ICV-Indicator,
        SAKR OLPL - SAK-Rekey On-Live-Peer-Loss,
        DP - Delay Protect, KS Prio - Key Server Priority

Policy            KS   DP    CO SAKR  ICVIND Cipher          Interfaces
Name              Prio          OLPL         Suite(s)        Applied
================================================================================
MKA-128           0    FALSE 0  FALSE TRUE   GCM-AES-128     Te0/0/5
```

show mka sessions

To display the active MACsec sessions on a Cisco IOS XE Catalyst SD-WAN device, use the **show mka sessions** command in privileged EXEC mode.

show mka sessions

Syntax Description This command has no keywords or arguments.

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	This command is supported for Cisco Catalyst SD-WAN.

Examples

This is sample output of the **show mka sessions** command.

```
Device# show mka sessions
Total MKA Sessions....... 1
      Secured Sessions... 1
      Pending Sessions... 0

=============================================================================================
Interface       Local-TxSCI          Policy-Name       Inherited          Key-Server

Port-ID         Peer-RxSCI           MACsec-Peers      Status             CKN

=============================================================================================
Te0/0/5         e8d3.22d3.2085/000d  MKA-128           NO                 NO

13              a03d.6e5d.037f/0045  1                 Secured            10
```

The following is a sample output from the **show mka sessions detail** command.

```
Device# show mka sessions detail
MKA Detailed Status for MKA Session
===================================
Status: SECURED - Secured MKA Session with MACsec

Local Tx-SCI..............e8d3.22d3.2085/000d
Interface MAC Address....e8d3.22d3.2085
MKA Port Identifier......13
Interface Name...........TenGigabitEthernet0/0/5
Audit Session ID.........
CAK Name (CKN)...........10
Member Identifier (MI)...DE832E171DCC70441E997F96
Message Number (MN)......134
EAP Role.................NA
Key Server...............NO
MKA Cipher Suite.........AES-256-CMAC

Latest SAK Status........Rx & Tx
Latest SAK AN............1
Latest SAK KI (KN).......811368FD2F9F9CC82C1894C800000012 (18)
Old SAK Status...........No Rx, No Tx
Old SAK AN...............0
Old SAK KI (KN)..........RETIRED (0)

SAK Transmit Wait Time...0s (Not waiting for any peers to respond)
SAK Retire Time..........0s (No Old SAK to retire)
SAK Rekey Time...........0s (SAK Rekey interval not applicable)

MKA Policy Name..........MKA-128
Key Server Priority......0
Delay Protection.........NO
Delay Protection Timer...........0s (Not enabled)

Confidentiality Offset...0
Algorithm Agility........80C201
SAK Rekey On Live Peer Loss........NO
Send Secure Announcement..DISABLED
SCI Based SSCI Computation....NO
SAK Cipher Suite.........0080C20001000001 (GCM-AES-128)
MACsec Capability........3 (MACsec Integrity, Confidentiality, & Offset)
MACsec Desired...........YES

# of MACsec Capable Live Peers............1
# of MACsec Capable Live Peers Responded..0

Live Peers List:
  MI                        MN          Rx-SCI (Peer)        KS        RxSA          SSCI
                                                             Priority  Installed
  ------------------------------------------------------------------------------------------
  811368FD2F9F9CC82C1894C8  379154      a03d.6e5d.037f/0045  0         YES            0

Potential Peers List:
  MI                        MN          Rx-SCI (Peer)        KS        RxSA          SSCI
                                                             Priority  Installed
  ------------------------------------------------------------------------------------------

Dormant Peers List:
  MI                        MN          Rx-SCI (Peer)        KS        RxSA          SSCI
                                                             Priority  Installed
  ------------------------------------------------------------------------------------------


MKA Detailed Status for MKA Session
===================================
```

```
Status: INITIALIZING - Searching for Peer (Waiting to receive first Peer MKPDU)

Local Tx-SCI.............. e8d3.22d3.2085/000d
Interface MAC Address.... e8d3.22d3.2085
MKA Port Identifier...... 13
Interface Name........... TenGigabitEthernet0/0/5
Audit Session ID.........
CAK Name (CKN)........... 11
Member Identifier (MI)... 6758F1CA5F050202DC742B03
Message Number (MN)...... 133
EAP Role................. NA
Key Server............... YES
MKA Cipher Suite......... AES-256-CMAC

Latest SAK Status........ Rx & Tx
Latest SAK AN............ 1
Latest SAK KI (KN)....... 811368FD2F9F9CC82C1894C800000012 (18)
Old SAK Status........... No Rx, No Tx
Old SAK AN............... 0
Old SAK KI (KN).......... RETIRED (0)

SAK Transmit Wait Time... 0s (Not waiting for any peers to respond)
SAK Retire Time.......... 0s (No Old SAK to retire)
SAK Rekey Time........... 0s (SAK Rekey interval not applicable)

MKA Policy Name.......... MKA-128
Key Server Priority...... 0
Delay Protection......... NO
Delay Protection Timer.......... 0s (Not enabled)

Confidentiality Offset... 0
Algorithm Agility........ 80C201
SAK Rekey On Live Peer Loss........ NO
Send Secure Announcement.. DISABLED
SCI Based SSCI Computation.... NO
SAK Cipher Suite......... 0080C20001000001 (GCM-AES-128)
MACsec Capability........ 3 (MACsec Integrity, Confidentiality, & Offset)
MACsec Desired........... YES

# of MACsec Capable Live Peers............ 0
# of MACsec Capable Live Peers Responded.. 0

Live Peers List:
  MI                      MN          Rx-SCI (Peer)        KS        RxSA          SSCI
                                                           Priority  Installed
  ----------------------------------------------------------------------------------------

Potential Peers List:
  MI                      MN          Rx-SCI (Peer)        KS        RxSA          SSCI
                                                           Priority  Installed
  ----------------------------------------------------------------------------------------

Dormant Peers List:
  MI                      MN          Rx-SCI (Peer)        KS        RxSA          SSCI
                                                           Priority  Installed
  ----------------------------------------------------------------------------------------
```

show mka statistics

To display MACsec statistics on a Cisco IOS XE Catalyst SD-WAN device, use the **show mka statistics** command in privileged EXEC mode.

show mka statistics

Syntax Description

This command has no keywords or arguments.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	This command is supported for Cisco Catalyst SD-WAN.

Examples

This is sample output of the **show mka statistics** command.

```
Device# show mka statistics interface TenGigabitEthernet 0/0/5
MKA Statistics for Session
==========================
Reauthentication Attempts.. 0

CA Statistics
   Pairwise CAKs Derived... 0
   Pairwise CAK Rekeys..... 0
   Group CAKs Generated.... 0
   Group CAKs Received..... 0

SA Statistics
   SAKs Generated.............. 0
   SAKs Rekeyed................ 0
   SAKs Received............... 1
   SAK Responses Received...... 0
   SAK Rekeyed as KN Mismatch.. 0

MKPDU Statistics
   MKPDUs Validated & Rx... 229
      "Distributed SAK".. 1
      "Distributed CAK".. 0
   MKPDUs Transmitted...... 231
      "Distributed SAK".. 0
      "Distributed CAK".. 0
```

show mka summary

To display MACsec statistics on a Cisco IOS XE Catalyst SD-WAN device, use the **show mka summary** command in privileged EXEC mode.

show mka summary

Syntax Description

This command has no keywords or arguments.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	This command is supported for Cisco Catalyst SD-WAN.

Examples

This is sample output of the **show mka summary** command.

```
Device# show mka summary
Total MKA Sessions....... 1
      Secured Sessions... 1
      Pending Sessions... 0

=============================================================================================================
Interface       Local-TxSCI          Policy-Name       Inherited          Key-Server

Port-ID         Peer-RxSCI           MACsec-Peers      Status             CKN

=============================================================================================================
Te0/0/5         e8d3.22d3.2085/000d  MKA-128           NO                 NO

13              a03d.6e5d.037f/0045  1                 Secured            10



MKA Global Statistics
=====================
MKA Session Totals
   Secured..................... 18
   Fallback Secured............ 0
   Reauthentication Attempts.. 0

   Deleted (Secured).......... 17
   Keepalive Timeouts......... 0

CA Statistics
   Pairwise CAKs Derived...... 0
   Pairwise CAK Rekeys........ 0
   Group CAKs Generated....... 0
   Group CAKs Received........ 0

SA Statistics
   SAKs Generated.............. 0
   SAKs Rekeyed................ 0
   SAKs Received............... 18
   SAK Responses Received...... 0
   SAK Rekeyed as KN Mismatch.. 0

MKPDU Statistics
   MKPDUs Validated & Rx...... 374465
      "Distributed SAK"..... 18
      "Distributed CAK"..... 0
   MKPDUs Transmitted......... 384191
      "Distributed SAK"..... 0
      "Distributed CAK"..... 0

MKA Error Counter Totals
========================
Session Failures
   Bring-up Failures................ 0
   Reauthentication Failures........ 0
   Duplicate Auth-Mgr Handle........ 0
```

```
SAK Failures
   SAK Generation.................. 0
   Hash Key Generation............. 0
   SAK Encryption/Wrap............. 0
   SAK Decryption/Unwrap........... 0
   SAK Cipher Mismatch............. 0

CA Failures
   Group CAK Generation............ 0
   Group CAK Encryption/Wrap....... 0
   Group CAK Decryption/Unwrap..... 0
   Pairwise CAK Derivation......... 0
   CKN Derivation.................. 0
   ICK Derivation.................. 0
   KEK Derivation.................. 0
   Invalid Peer MACsec Capability... 0

MACsec Failures
   Rx SC Creation.................. 0
   Tx SC Creation.................. 0
   Rx SA Installation.............. 0
   Tx SA Installation.............. 0

MKPDU Failures
   MKPDU Tx............................... 0
   MKPDU Rx ICV Verification.............. 0
   MKPDU Rx Fallback ICV Verification..... 0
   MKPDU Rx Validation.................... 0
   MKPDU Rx Bad Peer MN................... 0
   MKPDU Rx Non-recent Peerlist MN........ 0
SAK USE Failures
   SAK USE Latest KN Mismatch............. 0
   SAK USE Latest AN not in USE........... 0
```

show nat66 dia route

To show the NAT66 DIA route status information and to determine the number of NAT66 DIA-enabled routes, use the **show nat66 dia route** command in privileged EXEC mode.

show nat66 dia route

Syntax Description

This command has no arguments or keywords.

Command Default

No NAT66 DIA route status information is displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Examples

The following is a sample output from the **show nat66 dia route** command:

```
Device# show nat66 route-dia
Total interface NAT66 DIA enabled count [1]
route add [1] addr [2001:DB8:A14:19::] vrfid [2] prefix len [64]
route add [1] addr [2001:DB8:3D0:1::] vrfid [2] prefix len [64]
```

show nat64 map-e

To view information about the Network Address Translation (NAT64) Mapping of Address and Port Using Encapsulation (MAP-E) domain and associated parameters, use the **show nat64 map-e** command in privileged EXEC mode.

show nat64 map-e

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	This command was introduced.

Examples

The following is an example output for the **show nat64 map-e** command:

```
Device# show nat64 map-e
MAP-E Domain 9126
   Mode MAP
   Border-relay-address
      Ip-v6-address 2001:DB8::9
   Basic-mapping-rule
      Ip-v6-prefix 2001:DB8:A110::/48
      Ip-v4-prefix 10.1.1.0/24
      Port-parameters
         Share-ratio 16   Contiguous-ports 64   Start-port 1024
         Share-ratio-bits 4   Contiguous-ports-bits 6   Port-offset-bits 6
      Port-set-id 1
```

The output above shows the MAP-E domain and the associated parameters.

For more information on MAP-E with NAT64, see the *Cisco SD-WAN NAT Configuration Guide*.

Related Commands

Commands	Description
nt64 provisioning	Configure the MAP-E domain and parameters for NAT64.

show nat66 nd

To display the NAT66 discovery neighbors table, use the **show nat66 nd** command in privileged EXEC mode.

show nat66 nd

Syntax Description This command has no arguments or keywords.

Command Default No NAT66 discovery neighbors table is displayed.

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Examples The following is a sample output from the **show nat66 nd** command:

```
Device# show nat66 nd
NAT66 Neighbor Discovery

ND prefix DB:
  2001:DB8:A1:F::/80
  2001:DB8:A1:F:0:1::/80
  2001:DB8:A1:F:1::/64
  2001:DB8:A1:F:2::/64
  2001:DB8:A1:F:3::/64

ipv6 ND entries:
  2001:DB8:A1:F::F
  2001:DB8:A1:F::11
```

show nat66 prefix

To show the status of the NAT66 prefix configuration and to display the NAT66 configured prefixes, use the **show nat66 prefix** command in privileged EXEC mode.

show nat66 prefix

Syntax Description This command has no arguments or keywords.

Command Default No IPv6 configured prefixes are displayed.

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Examples The following is a sample output from the **show nat66 prefix** command, and shows the NAT66 prefixes that were configured:

```
Device# show nat66 prefix
Prefixes configured: 1
NAT66 Prefixes
Id: 1 Inside 2001:DB8:AB01::/64 Outside 2001:DB8:AB02::/64
```

show nat66 statistics

To verify the NAT66 interface and global configuration, use the **show nat66 statistics** command in privileged EXEC mode.

show nat66 statistics

Syntax Description This command has no arguments or keywords.

Command Default No NAT66 interface and global configuration statistics are displayed.

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command is supported for Cisco Catalyst SD-WAN.

Examples The following is a sample output from the **show nat66 statistics** command and shows the packet headers that were translated.

```
Device# show nat66 statistics
NAT66 Statistics

Global Stats:
   Packets translated (In -> Out)
      : 7
   Packets translated (Out -> In)
      : 7
```

show object-group

To display object group configuration, use the **show object-group** command in privileged EXEC mode.

show object-group name *object-group-name*

Syntax Description

name *object-group-name*	(Optional) Displays information for a specific object group.

Command Default Information for all the object groups is displayed.

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Use the **show object-group** command to display configurations for all object groups or just for a specific object group.

Examples

The following is example output from the **show object-group** command:

```
Device# show object-group name Zone1_to_Zone1-seq-Rule_1-geo-dstn-og_
GEO object group Zone1_to_Zone1-seq-Rule_1-geo-dstn-og_
country FRA
```

show policy-firewall session platform detail

To display display detailed information about firewall sessions on a Cisco IOS XE Catalyst SD-WAN device, particularly when high availability is involved, use the **show policy-firewall session platform detail** command in privileged EXEC mode.

show policy-firewall session platform detail

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.15.1a	This command is supported for Cisco Catalyst SD-WAN.

Usage Guidelines

Use the **show policy-firewall session platform detail** to display detailed information about firewall sessions on the platform, particularly when high availability is involved. This command is used to gather comprehensive data about active firewall sessions, including session states, counters, and other important metrics.

Examples

The following is sample output from the **show policy-firewall session platform detail** command.

```
Device# show policy-firewall session platform detail
[s=session i=imprecise channel c=control channel d=data channel u=utd inspect A/D=appfw
action allow/deny]
Session ID:0x100000B7 192.168.11.10 34157 10.0.12.131 80 proto 6 (1:1:1:1) (3:0x3000050:http)
 [sc]
pscb : 0x156da640, key1_flags: 0x00000000
bucket : 34590, prev 0x0, next 0x0 fw_flags: 0x01800000 0x20c06a21,
Flattened-AVC HA-AVC
Root Protocol-TCP Initiator Alert Proto-State:Timewait Session-db HA-create Max-session
icmp_error count 0 ureachable arrived: no
scb state: active, nxt_timeout: 100, refcnt: 1 NBAR verdict count 0
ha nak cnt: 0, rg: 1
hostdb: 0x0, L7: 0x0, stats: 0x160ebfc0, child: 0x0
isn: 1826966309 last ack: 987459709 next seq: 1826966394 wnd_size: 2169783926
wnd_scale: 29200
isn: 987459708 last ack: 987459708 next ack: 987459708 wnd_size: 2169783926
wnd_scale: 65535
tcp_flags: 0x00000000 : : proto: 0018: l7 ooo drop 0x010 l7_prot 0x12 - http
```

```
root scb: 0x0 act_blk: 0x160e3f00
ingress/egress intf: GigabitEthernet3.101 (65530), GigabitEthernet1 (65530)
current time 284036397554511 create tstamp: 283915721110241 last access: 284035994128283
now 284036397556361 csec left
nat_out_local_addr:port: 10.0.12.131:80
nat_in_global_addr:port: **********
ip6: addr1 :: addr2 ::
key ip4: addr1 10.0.12.131:80 addr2 192.168.11.10:34157
syncookie fixup: 0x0, halfopen linkage: 0x0 0x0
cxsc_cft_fid: 0x00000000
tw timer: 0x00000000 0x00000000 0x00000000 0x14f53101
domain_ab1 0x0 l4 per filter stats 0x0 avc class id 0x3 http SGT: 0 DGT: 0
NAT handles 0x11194110 0x00000000
FlowDB in2out 0x00000000 alloc_epoch 0 out2in 0x00000000 alloc_epoch 0 ppe tid 0
icmp_err_time 0 utd_context_id 0, classification epoch scb: 0x1 actblk :0x1 avc class stats
 0x0
VPN id src 1, dst 0
zone pair ZP_ZONE_1_untrusted_ZON_47132514 class
ZONE_1_TO_UNTRUSTED-seq-SEQUENCE-829881385-cm_
```

show performance monitor cache

To view performance monitor cache details, use the **show performance monitor cache** command in privileged EXEC mode.

show performance monitor cache [**detail** | **format** { **csv** | **table** | **record** }]

show performance monitor cache [**monitor** *monitor-name*]

Syntax Description

detail	(Optional) Displays detailed cache information.
format	Displays cache information in one of the formats specified: • CSV • record • table
monitor *monitor-name*	Displays cache information for the specified monitor name.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	This command can be used to view performance monitor cache details in controller mode.

Example

The following is sample output from the **show performance monitor cache** command:

```
Device# show performance monitor cache
```

```
Monitor: CISCO-media_ipv4

 Data Collection Monitor:

  Cache type:                           Synchronized (Platform cache)
  Cache size:                                  4000
  Current entries:                                0

  Flows added:                                    0
  Flows aged:                                     0
  Synchronized timeout (secs):                   60


 Monitor: 175_SDWAN-art_ipv4

 Data Collection Monitor:

  Cache type:                           Synchronized (Platform cache)
  Cache size:                                 11250
  Current entries:                                0

  Flows added:                                    0
  Flows aged:                                     0
  Synchronized timeout (secs):                   60
```

show performance monitor context

To view information about performance monitor configuration for a specified context, use the **show performance monitor context** command in privileged EXEC mode.

show performance monitor context *context* [**configuration** | **exporter** | **interface** | **summary** | **traffic-monitor**]

Syntax Description

context	Name of the performance monitor context. If a context name is not specified, all contexts are displayed.

configuration	(Optional) Displays all configuration of the specified context. This command can be used to convert the auto configuration to the traditional configuration.
exporter	(Optional) Displays the operational information about the exporters attached to the specified context.
interface	(Optional) Displays information about the performance monitor interface.
summary	(Optional) Displays information about the enabled traffic monitors and the interfaces to which they are attached.
traffic-monitor	(Optional) Displays information about the traffic-monitors configured for the performance monitor.

Command Default

When none of the optional keywords and arguments is specified, information is displayed for all contexts.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	This command can be used in Cisco SD-WAN controller mode.

Usage Guidelines

Use the **show performance monitor context** command to view all configuration for the specified context.

Example

The following are sample outputs from the **show performance monitor context** command:

```
Device# show performance monitor context CISCO-MONITOR summary

================================================================================

|                              CISCO-MONITOR                                   |

================================================================================

Description: User defined


Based on profile: sdwan-performance


Coarse-grain NBAR based profile


Configured traffic monitors

============================

 application-response-time:

 media: class-and match_audio
```

```
Attached to Interfaces

=====================

 Tunnel1
```

The following sample output shows exporter details for the performance monitor context named CISCO-MONITOR.

```
Device# show performance monitor context CISCO-MONITOR exporter

================================================================================

|                  Exporters information of context CISCO-MONITOR                |

================================================================================


Flow Exporter CISCO-MONITOR:

  Description:              performance monitor context CISCO-MONITOR exporter

  Export protocol:          IPFIX (Version 10)

  Transport Configuration:

    Destination type:       IP

    Destination IP address: 10.75.212.84

    Source IP address:      10.74.28.19

    Source Interface:       GigabitEthernet0/0/0

    Transport Protocol:     UDP

    Destination Port:       2055

    Source Port:            63494

    DSCP:                   0x0

    TTL:                    255

    Output Features:        Used

  Options Configuration:

    interface-table (timeout 600 seconds) (active)

    sampler-table (timeout 600 seconds) (active)

    application-table (timeout 600 seconds) (active)

    sub-application-table (timeout 600 seconds) (active)

    application-attributes (timeout 600 seconds) (active)

    tunnel-tloc-table (timeout 600 seconds) (active)

Flow Exporter CISCO-MONITOR:
```

```
Packet send statistics (last cleared 04:13:19 ago):
  Successfully sent:         10270                 (13709142 bytes)

Client send statistics:
  Client: Option options interface-table
    Records added:           312
      - sent:                312
    Bytes added:             31824
      - sent:                31824

  Client: Option options sampler-table
    Records added:           28
      - sent:                28
    Bytes added:             1344
      - sent:                1344

  Client: Option options application-name
    Records added:           38766
      - sent:                38766
    Bytes added:             3217578
      - sent:                3217578

  Client: Option sub-application-table
    Records added:           858
      - sent:                858
    Bytes added:             144144
      - sent:                144144

  Client: Option options application-attributes
    Records added:           38038
      - sent:                38038
    Bytes added:             9813804
```

```
    - sent:                9813804


Client: Option options tunnel-tloc-table
  Records added:           26
    - sent:                26
  Bytes added:             1352
    - sent:                1352


Client: MMA EXPORTER GROUP MMA-EXP-1
  Records added:           0
  Bytes added:             0




Client: Flow Monitor CISCO-MONITOR-art_ipv4
  Records added:           0
  Bytes added:             0


Client: Flow Monitor CISCO-MONITOR-media_ipv4
  Records added:           0
  Bytes added:             0
```

show platform hardware qfp active classification class-group-manager class-group client cce name

To view an optimized policy for a firewall, use the **show platform hardware qfp active classification class-group-manager class-group client cce name** command in user EXEC or privileged EXEC mode.

show platform hardware qfp active classification class-group-manager class-group client cce name

Command Default

None

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

The following is sample output from the **show platform hardware qfp active classification class-group-manager class-group client cce name** command.

```
Device# show platform hardware qfp active classification class-group-manager class-group
client cce name FW_POLICY1-opt
class-group [cce-cg:12272256] FW_POLICY1-opt (classes: 2)
 clients: fw
 fields: ipv4_og_src:4 any:1 dst_geo_id:4  (100000:0:0:200:100000:00000000)
  (2097151) class: logical-expression [12272256.2734225] FW_POLICY1-seq-1-cm_ (filters: 1)
          lexp: LOG-EXP: [1]
    (1) filter: generic [12272256.2734225.1] (rules: 4)
      (1) rule: generic  [12272256.2734225.1.1] (permit)
         match ipv4_og_src 1
         match dst_geo_id 0xc24 / 0xffff
      (2) rule: generic  [12272256.2734225.1.2] (permit)
         match ipv4_og_src 1
         match dst_geo_id 0x1164 / 0xffff
      (3) rule: generic  [12272256.2734225.1.3] (permit)
         match ipv4_og_src 1
         match dst_geo_id 0xe2a / 0xffff
      (4) rule: generic  [12272256.2734225.1.4] (permit)
         match ipv4_og_src 1
         match dst_geo_id 0x1a9a / 0xffff
  (4294967295) class: logical-expression [12272256.1593] class-default (filters: 1)
          lexp: LOG-EXP: [1]
    (1) filter: generic [12272256.1593.1] (rules: 1)
      (1) rule: generic  [12272256.1593.1.1] (permit)
         match any
```

show platform hardware qfp active classification class-group-manager class-group client sdwan

To view the policy name or group-id in class-group-manager and to get the detail info, use the **show platform hardware qfp active classification class-group-manager class-group client sdwan** command in privileged EXEC mode.

show platform hardware qfp active classification class-group-manager class-group client sdwan { **all** | **name** *class-group-name* | *class-group-id* }

Syntax Description

all	All class group.
name *class-group-name*	Name of the class group.
class-group-id	Class group id. Range: 0 to 4294967295

Command Default

None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This command was introduced.

Usage Guidelines This command displays information that helps you to troubleshoot related issues about policy name or group-id in class-group-manager.

Examples The following is a sample output from the **show platform hardware qfp active classification class-group-manager class-group client sdwan** command:

```
Device# show platform hardware qfp active classification class-group-manager class-group
client sdwan all
QFP classification class client all group
  class-group [SDWAN:21] DATA_POLICY-vpn_1
  class-group [SDWAN:22] AAR_POLICY-vpn_1

Device# show platform hardware qfp active classification class-group-manager class-group
client sdwan 21
class-group [sdwan-cg:21] DATA_POLICY-vpn_1 (classes: 8)
 clients:
 fields: l4_dst:2 ipv4_og_src:8 ipv4_og_dst:24 ipv6_og_src:1 ipv6_og_dst:2 any:1
ip_protocol_range:2 dns_request:4 dns_response:4
og_usr_app_id:6  (300100:600:0:100200:1300:00000000)
  (11) class: logical-expression [21.11] DATA_POLICY-vpn_1-seq-11 (filters: 7)
          lexp: LOG-EXP: ,
    (1) filter: generic [10.11.1] (rules: 1)
      (1) rule: generic  [10.11.1.1] (permit)
         match l4_dst range 5060 5060

Device# show platform hardware qfp active classification class-group-manager class-group
client sdwan name AAR_POLICY-vpn_1
class-group [sdwan-cg:22] AAR_POLICY-vpn_1 (classes: 6)
 clients:
 fields: ip_tos:1 l4_dst:1 ipv4_og_src:6 ipv4_og_dst:12 ipv6_og_src:1 ipv6_og_dst:2 any:1
ip_protocol_range:1 dns_request:3 dns_response:3
og_usr_app_id:4  (300110:600:0:100200:1300:00000000)
  (1) class: logical-expression [22.1] AAR_POLICY-vpn_1-seq-1 (filters: 10)
          lexp: LOG-EXP: ,
    (1) filter: generic [10.1.1] (rules: 2)
      (1) rule: generic  [10.1.1.1] (permit)
         match ipv4_og_src 57419
      (2) rule: generic  [10.1.1.2] (permit)
         match ipv4_og_src 57420
    (2) filter: generic [10.1.2] (rules: 6)
      (1) rule: generic  [10.1.2.1] (permit)
         match ipv4_og_dst 57421
      (2) rule: generic  [10.1.2.2] (permit)
```

show platform hardware qfp active classification class-group-manager object-group

To get the name or id of the tag membership in class-group-manager, use the **show platform hardware qfp active classification class-group-manager object-group** command in privileged EXEC mode.

show platform hardware qfp active classification class-group-manager object-group { **all** | **name** *object-group-name* | **type** { **IPv4** | **IPv6** | **ref_ace_v4** } }

Syntax Description

all	All object group.
name *object-group-name*	Name of the Object-Group.
type	Type of the Object-Group.
ref_ace_v4	Reflect ACE V4.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This command was introduced.

Usage Guidelines

This command displays information that can help you to troubleshoot issues about the tag membership in class-group-manager.

Examples

The following is a sample output from the **show platform hardware qfp active classification class-group-manager object-group** command, use to verify the object-group IDs.

```
Device# show platform hardware qfp active classification class-group-manager object-group
all
QFP classification object-group all
  multicast_pfx_t:57417  Type: IPV4  No. of Entries: 1
  pfx1_t:57418  Type: IPV4  No. of Entries: 1
  pfx21_t:57419  Type: IPV4  No. of Entries: 1
  pfx22_t:57420  Type: IPV4  No. of Entries: 2
  pfx31_t:57421  Type: IPV4  No. of Entries: 5
  pfx32_t:57422  Type: IPV4  No. of Entries: 1
  pfx33_t:57423  Type: IPV4  No. of Entries: 1
  pfx34_t:57424  Type: IPV4  No. of Entries: 1
  pfx35_t:57425  Type: IPV4  No. of Entries: 1
  pfx36_t:57426  Type: IPV4  No. of Entries: 1
  subnet_0_t:57427  Type: IPV4  No. of Entries: 1
  v6_pfx1_t_v6:57428  Type: IPV6  No. of Entries: 1
  v6_pfx21_t_v6:57429  Type: IPV6  No. of Entries: 2
  v6_pfx22_t_v6:57430  Type: IPV6  No. of Entries: 3
  apps_facebook_type_app_id_t:57431  Type: USR-APPID  No. of Entries: 2
  apps_ms_type_app_id_t:57432  Type: USR-APPID  No. of Entries: 6
  apps_webex_type_app_id_t:57433  Type: USR-APPID  No. of Entries: 6
  apps_zoom_type_app_id_t:57434  Type: USR-APPID  No. of Entries: 1
```

show platform hardware qfp active classification feature message all

To display recent Classification Feature Manager (CFM) syslog messages on a Cisco Quantum Flow Processor (QFP), use the **show platform hardware qfp active classification feature message** command in privileged EXEC mode.

show platform hardware qfp active classification feature message { **all** | **clear** }

Syntax Description

all	Displays all the CFM syslog message buffer.
clear	Clears the syslog circular buffer.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	This command was introduced.

Usage Guidelines

Use this command to debug CFM related issues in a QFP by analyzing the feature manager messages.

This command displays the CFM syslog message buffer. A message buffer can save up to 300 messages in a fixed-size buffer. The messages are displayed in the last in, first out (LIFO) order.

Example

The following example displays the recent CFM syslog messages.

```
Device# show platform hardware qfp active active classification feature message all
Sep 24 08:35:52.670: : CPP_FM_CLIENT_WARNING: ATTACH request failed for acl client id[acl:32]
 name[lab-lenient1] label[0]. Error code: 0x1c(No space left on device)


Sep 24 08:35:50.763: : CPP_FM_SW_TCAM_WARNING: CACE EXMEM allocation fail: acl client
id[acl-cg:32] name[lab-lenient1] attempted to allocate114971756 bytes


Sep 24 04:58:13.425: : CPP_FM_CLIENT_WARNING: ATTACH request failed for qos client
id[cce:8265536] name[inputPolicy] label[0]. Error code: 0x71(No route to host)


Sep 24 04:58:13.424: : CPP_FM_TCAM_CE_WARNING: Failed to select tcam key: could not find
matching key format for qos client id[cce:8265536] name[inputPolicy] field
bit-map[18050:0:300000:200:0:00000000]
```

show platform hardware qfp active classification feature-manager exmem-usage

To display the External Memory Manager (EXMEM) usage on a Cisco Quantum Flow Processor (QFP), use the **show platform hardware qfp active classification feature-manager exmem-usage** command in privileged EXEC mode.

show platform hardware qfp active classification feature-manager exmem-usage sorted

Syntax Description

sorted	Displays the memory usage sorted at the policy level. The policy with the highest EXMEM usage appears first.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	This command was introduced.

Usage Guidelines

Use this command to display the EXMEM usage at the client level and at the policy level.

Example

The following example shows how to display the EXMEM memory usage for various clients. The display order is according to the client ID.

```
Device# show platform hardware qfp active active classification feature-manager exmem-usage

EXMEM Usage Information

Total exmem used by CACE: 39668

Client       Id   Total VMR     Total Usage   Total%   Alloc     Free
-------------------------------------------------------------------------
acl           0      11           2456          6         88       84
qos           2     205          31512         79          7        5
fw            4       8            892          2          2        1
obj-group    39      82           4808         12          5        2
```

The following example shows how to display the memory usage sorted at the policy level. The policy with the highest EXMEM usage appears first.

```
Device# show platform hardware qfp active active classification feature-manager exmem-usage
 sorted

EXMEM Usage Information

Total VMR entries used by CACE: 306
```

```
Total exmem used by CACE: 39668

CG-Id               Name                Client          VMR        Usage       Label
-------------------------------------------------------------------------------------
cce:8265536         inputPolicy          QOS            198        30680       107
obj-group:7            ---               OBJ-GROUP       80         3928       103
cce:13747824         fw-policy           FW               8          892        26
cce:482000           odm                 QOS              7          832       102
acl:29               og_acl              ACL              4          764       105
acl:30               og_acl_1            ACL              4          764       104
acl:5                acl111              ACL              2          488        83
acl:6                acl112              ACL              1          440        84
obj-group:5            ---               OBJ-GROUP        1          440        80
obj-group:3            ---               OBJ-GROUP        1          440        77
```

show platform hardware qfp active classification feature-manager statistics

To display Classification Feature Manager (CFM) error statistics, use the **show platform hardware qfp active classification feature-manager statistics** command in privileged EXEC mode.

This command **show platform hardware qfp active classification feature-manager statistics** has been added to admin-tech. For more information on **admin-tech** command, see request admin-tech

show platform hardware qfp active classification feature-manager statistics

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

Use this command for troubleshooting a client in a QFP by analysing the feature manager requests statistics.

Example

The following example shows how to display the CFM error statistics.

```
Device# show platform hardware qfp active active classification feature-manager statistics
Client        Id  Attach      Err     ReplaceCG   Err     Edit        Err     Release
Err     Detach      Err     RelToTCAM   Err
     Drop

obj-group     39  2           0       0           0       0           0       0
0       0           0       0           0
     0
sdwan-approu  46  1           0       0           0       1           0       1
0       0           0       0           0
```

```
     0
sdwan-dp       47  1            0       0           0       1           0       1
0       0            0       0           0
     0
```

show platform hardware qfp active feature acl control

To display whether Security Group Access Control List (SGACL) logging is enabled or disabled, use the **show platform hardware qfp active feature acl control** command in privileged EXEC mode.

show platform hardware qfp active feature acl control

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.15.1a	This command is supported for Cisco Catalyst SD-WAN.

Usage Guidelines

Use the **show platform hardware qfp active feature acl control** to display whether SGACL logging is enabled or disabled.

Examples

The following is sample output from the **show platform hardware qfp active feature acl control** command. In this example, SGACL logging is enabled.

```
Device# show platform hardware qfp active feature acl control
Stats Poll Period: 0
Stats Entry Size: 16
Ha Init: 1
Fm Ready: 0
IPv4 Logging Threshold: 2147483647
IPv4 Logging Interval: 0
IPv6 Logging Threshold: 350000
IPv6 Logging Interval: 0
Maximum Aces Per Acl: 256000
Stats Update size: 180
Maximum Entries: 0
Maximum Entries per Classifier: 0
Result Bit Size: 0
Result Start Bit Pos: 0
Maximum Profiles: 0
Maximum Blocks per Profile: 0
Device Select: 0
Maximum Tree Depth: 0
Dimention: 0
Number Cuts: 0
HSL Support: TRUE // sgacl hsl logging is enabled
HSL Force Disable: FALSE
```

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

Field	Description
Stats Poll Period	The interval (in seconds) at which statistics are polled. A value of 0 indicates that polling is disabled.
Stats Entry Size	The size of each statistics entry in bytes.
Ha Init	Indicates whether High Availability (HA) initialization has been completed. A value of 1 means it is initialized.
Fm Ready	Indicates whether the Forwarding Manager (FM) is ready. A value of 0 means it is not ready.
IPv4 Logging Threshold	The threshold for logging IPv4 packets.
IPv4 Logging Interval	The interval (in seconds) for logging IPv4 packets. A value of 0 indicates that interval-based logging is disabled.
IPv6 Logging Threshold	The threshold for logging IPv6 packets.
IPv6 Logging Interval	The interval (in seconds) for logging IPv6 packets. A value of 0 indicates that interval-based logging is disabled.
Maximum Aces Per Acl	The maximum number of Access Control Entries (ACEs) allowed per ACL.
Stats Update size	The size of the statistics update in bytes.
Maximum Entries	The maximum number of entries allowed. A value of 0 may indicate that there is no set limit or that the feature is disabled.
Maximum Entries per Classifier	The maximum number of entries allowed per classifier. A value of 0 may indicate that there is no set limit or that the feature is disabled.
Result Bit Size	The size of the result bit field. A value of 0 may indicate that this feature is not in use.
Result Start Bit Pos	The starting bit position for the result field. A value of 0 may indicate that this feature is not in use.
Maximum Profiles	The maximum number of profiles allowed. A value of 0 may indicate that there is no set limit or that the feature is disabled.
Maximum Blocks per Profile	The maximum number of blocks allowed per profile. A value of 0 may indicate that there is no set limit or that the feature is disabled.
Device Select	The device selection parameter. A value of 0 may indicate a default or unspecified device.
Maximum Tree Depth	The maximum depth of the tree structure used for ACL processing. A value of 0 may indicate that this feature is not in use.
Dimension	Refers to the dimensionality of the ACL processing structure. A value of 0 may indicate that this feature is not in use.

Field	Description
Number Cuts	The number of cuts or divisions used in the ACL processing structure. A value of 0 may indicate that this feature is not in use.
HSL Support	Indicates whether HSL is supported on the device. A value of TRUE means HSL is supported and enabled.
HSL Force Disable	Indicates whether HSL is forcibly disabled. A value of FALSE means HSL is not forcibly disabled and can be used.

show platform hardware qfp active feature acl dp hsl configuration

To display the configuration for Security Group Access Control List (SGACL) HSL, use the **show platform hardware qfp active feature acl dp hsl configuration** command in privileged EXEC mode.

show platform hardware qfp active feature acl dp hsl configuration

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.15.1a	This command was introduced.

Usage Guidelines

Use the **show platform hardware qfp active feature acl dp hsl configuration** to display the configuration for SGACL HSL as set up on the device.

Examples

The following is sample output from the **show platform hardware qfp active feature acl dp hsl configuration** command .

```
Device# show platform hardware qfp active feature acl dp hsl configuration
ACL DP HSL Config:
HSL Supported: TRUE
HSL SGACL Enabled: TRUE
SGACL HSL Setup:
Handle Session/Instance: 127/63
Version: 9
Dest Type: 3
HSL Enable: TRUE
HSL BackPressure Enable: FALSE
Base Memory Addr: <0xpXXXX>
Memory Size (bytes): 147560
Max Records: 1024
Record Threshold: 256
Memory Threshold (bytes): 32768
Record Timeout (ms): 512
Export Timeout (ms): 4
MTU Size (bytes): 1450
```

```
Template Refresh Timer: 0
Template Refresh Packets: 0
Source Id: 0x404”
Max Record Size (bytes): 104
```

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

Field	Description
HSL Supported	Indicates that HSL is supported on the device.
HSL SGACL Enabled	Indicates that HSL for SGACL logging is enabled on the device.
Handle Session/Instance	Represents the session and instance handle numbers used for HSL configuration.
Version	Indicates the version of the HSL configuration being used.
Dest Type	Specifies the destination type for the HSL logs. This could refer to the type of logging destination, such as a syslog server or a specific logging format.
HSL Enable	Indicates that HSL is enabled for SGACL logging.
HSL BackPressure Enable	Indicates whether backpressure is enabled for HSL. Backpressure is a flow control mechanism to prevent buffer overflow. A value of FALSE means it is not enabled.
Base Memory Addr	The base memory address used for HSL logging. This is a placeholder for the actual memory address.
Memory Size (bytes)	The total memory size allocated for HSL logging, in bytes.
Max Records	The maximum number of log records that can be stored in the HSL memory.
Record Threshold	The threshold number of records that triggers certain actions, such as exporting logs.
Memory Threshold (bytes)	The memory usage threshold, in bytes, that triggers certain actions, such as exporting logs.
Record Timeout (ms)	The timeout period, in milliseconds, for log records before they are exported.
Export Timeout (ms)	The timeout period, in milliseconds, for exporting log records.
MTU Size (bytes)	The Maximum Transmission Unit (MTU) size, in bytes, for HSL log packets. This defines the largest size of a packet that can be transmitted.
Template Refresh Timer	The interval, in seconds, for refreshing the HSL template. A value of 0 indicates that template refresh is disabled.
Template Refresh Packets	The number of packets after which the HSL template is refreshed. A value of 0 indicates that template refresh based on packet count is disabled.
Source Id	The source identifier used for HSL logging. This is a hexadecimal value that uniquely identifies the source of the logs.
Max Record Size (bytes)	The maximum size, in bytes, of a single log record.

show platform hardware qfp active feature acl dp hsl statistics

To display the logging statistics for Security Group Access Control List (SGACL) HSL from the device, use the **show platform hardware qfp active feature acl dp hsl statistics** command in privileged EXEC mode.

show platform hardware qfp active feature acl dp hsl statistics

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.15.1a	This command was introduced.

Usage Guidelines

Use the **show platform hardware qfp active feature acl dp hsl statistics** to display the logging statistics for SGACL HSL from the device.

Examples

The following is sample output from the **show platform hardware qfp active feature acl dp hsl statistics** command.

```
Device# show platform hardware qfp active feature acl dp hsl statistics
ACL DP HSL Statistics:
HSL Supported: TRUE
HSL SGACL Enabled: TRUE
SGACL Export Statistics
-----------------------
Records sent (to HSL): 2
Records dropped (before HSL): 0
Record alloc failures: 0
Records dropped flag: Off
Records sent (by HSL): 0
Records dropped (by HSL): 0
HSL packets dropped flag: Off
HSL buffer flow-on (count): 0
SGACL HSL Statistics
--------------------
Records exported: 2
Packets exported: 2
Bytes exported: 168
Dropped records: 0
Dropped packets (inc. Punt drops): 0
Dropped bytes: 0
```

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

Field	Description
HSL Supported: TRUE	Indicates that High Speed Logging (HSL) is supported on the device.
HSL SGACL Enabled: TRUE	Indicates that HSL for SGACL logging is enabled on the device.
Records sent (to HSL)	The number of SGACL log records that have been sent to the HSL system for processing.

Field	Description
Records dropped (before HSL)	The number of SGACL log records that were dropped before reaching the HSL system.
Record alloc failures	The number of times the system failed to allocate memory for SGACL log records.
Records dropped flag	Indicates whether the flag for dropping records is active. "Off" means no records are currently being dropped due to this flag.
Records sent (by HSL)	The number of SGACL log records that have been successfully sent by the HSL system.
Records dropped (by HSL)	The number of SGACL log records that were dropped by the HSL system.
HSL packets dropped flag	Indicates whether the flag for dropping HSL packets is active. **Off**means no HSL packets are currently being dropped due to this flag.
HSL buffer flow-on (count)	The number of times the HSL buffer has been in a flow-on state, which typically indicates high buffer usage or potential overflow conditions.
Records exported	The total number of SGACL log records that have been exported by the HSL system.
Packets exported	The total number of packets associated with the exported SGACL log records.
Bytes exported	The total number of bytes associated with the exported SGACL log records.
Dropped records	The total number of SGACL log records that have been dropped during the export process.
Dropped packets (inc. Punt drops)	The total number of packets that have been dropped during the export process, including those dropped due to punt conditions (packets that are forwarded to the control plane for processing).
Dropped bytes	The total number of bytes that have been dropped during the export process.

show platform hardware qfp active feature bfd datapath

To display information about the BFD datapath summary in a data plane, use the **show platform hardware qfp active feature bfd datapath** command in privileged EXEC (#).

show platform hardware qfp active feature bfd datapath [**sdwan-summary**] [**sdwan ld** *sdwan-ld*]

Syntax Description

sdwan-summary	Displays the summary for a specific Cisco SD-WAN device.

sdwan ld *sdwan-ld*	Displays the status for a specific SDWAN instance. Specify Cisco SD-WAN local discriminator value. Range:1 to 65531

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.15.1a	This command was introduced.

Usage Guidelines

Use the command **show platform hardware qfp active feature bfd datapath sdwan-summary** to find out the local discriminator value for a particular BFD session. Then, you can run **show platform hardware qfp active feature bfd datapath sdwan ld** *sdwan ld* to display information about BFD datapath in the data plane for that session.

Examples

The following sample output displays the summary of BFD sessions in a data plane:

```
Device# show platform hardware qfp active feature bfd datapath sdwan summary
Total number of session: 12
LD       SrcIP      DstIP          TX         RX     Encap    State  AppProbe    AdjId
20001  192.168.4.0  172.16.17.1   183527   182839   IPSEC    Up     YES      GigabitEthernet1
 (0xf810000f)
20002  172.16.1.0   172.16.17.1   183535   182850   IPSEC    Up     YES      GigabitEthernet3
 (0xf810001f)
20003  192.168.4.1  192.168.4.0   182429   182003   IPSEC    Up     YES      GigabitEthernet1
 (0xf810002f)
20004  172.16.4.0   192.168.5.0   183129   181973   IPSEC    Up     YES      GigabitEthernet3
 (0xf810003f)
20005  192.168.4.1  192.168.4.0   175600   174575   IPSEC    Up     YES      GigabitEthernet1
 (0xf810004f)
20006  172.16.0.0   192.168.5.0   175596   174569   IPSEC    Up     YES      GigabitEthernet3
 (0xf810005f)
20007  192.168.4.0  192.168.3.3   183550   182864   IPSEC    Up     YES      GigabitEthernet1
 (0xf810006f)
20008  172.16.1.1   192.168.3.3   183568   182880   IPSEC    Up     YES      GigabitEthernet3
 (0xf810007f)
20009  192.168.4.0  192.168.1.1   182718   182410   IPSEC    Up     YES      GigabitEthernet1
 (0xf810008f)
20010  172.16.17.1  192.168.1.1   183381   182440   IPSEC    Up     YES      GigabitEthernet3
 (0xf810009f)
20011  192.168.5.0  172.16.1.0    175548   174523   IPSEC    Up     YES      GigabitEthernet1
 (0xf81000af)
20012  172.16.1.2   172.16.1.1    175572   174547   IPSEC    Up     YES      GigabitEthernet3
 (0xf81000bf)
```

The following sample output displays the BFD datapath information in data plane:

```
Device# show platform hardware qfp active feature bfd datapath sdwan ld 20008
LD                    : 20008
My Private IP         : 172.16.1.1
Remote Private IP     : 192.168.4.0
Tx Stats              : 183600
Rx Stats              : 182912
```

```
Encap Type            : IPSEC
State                 : Up
AppProbe              : YES
IPSec Out SA ID       : 0x24000024
Tunnel Rec ID         : 8
IfName                : GigabitEthernet3 (0xf810007f)
Uidb                  : 65528
Config Tx Timer       : 1000000
Conig Detect Timer    : 7000000
Actual Tx Timer       : 1000000
Actual Detect Timer   : 7000000
My Pub IP             : 172.16.1.0
My Pub Port           : 12346
My Symmetric NAT IP   : 0.0.0.0
My Symmetric NAT Port : 0
Remote public IP      : 192.168.4.0
Remote public Port    : 12346
MTU(config), Actual   : 1442, 1442
Farend PMTU           : 1442
My Capabilities       : 0x160
Remote Capabilities   : 0x160
SDWAN BFD flags       : ||||||| (0x0)
local_color           : 4
Ipsec Overhead        : 38
PFR stats for SLA default (addr:0xf14c02a0)
Number of pkts  : 524
Loss Count      : 0
Latency(1/16ms) : 416
Jitter(1/16ms)  : 832
Following are SDWAN stats
Echo Tx         : 182005
req          : 91415
reply        : 90590
Echo Rx         : 181317
req          : 90590
reply        : 90727
PMTU Tx         : 1595
PMTU RX         : 1595
AppProbeIDValid  NextProbeID StatAddr #Packets  Loss Latency(1/16ms) Jitter(1/16ms)
1         N         0        f14c02c0    0       0       0             0
2         N         0        f14c02e0    0       0       0             0
3         N         0        f14c0300    0       0       0             0
4         N         0        f14c0320    0       0       0             0
5         N         0        f14c0340    0       0       0             0
6         N         0        f14c0360    0       0       0             0
```

show platform hardware qfp active feature bfd datapath

To display information about BFD datapath in the data plane, use the **show platform hardware qfp active feature bfd datapath sdwan ld** command in privileged EXEC (#).

show platform hardware qfp active feature bfd datapath [**sdwan ld** *sdwan-ld*]

Syntax Description

sdwan ld *sdwan-ld*	Displays the status for a specific SDWAN instance. Specify Cisco SD-WAN ld value. Range:1 to 65531

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.15.1a	This command was introduced.

Usage Guidelines

Use the command **show platform hardware qfp active feature bfd datapath sdwan-summary** to find out the local discriminator (LD) value for a particular BFD session. Then, you can run **show platform hardware qfp active feature bfd datapath sdwan ld** *sdwan ld* to display information about BFD datapath in the data plane for that session. For more information, see command **show platform hardware qfp active feature bfd datapath sdwan-summary**.

Examples

The following sample output displays the BFD datapath information in data plane:

```
Device# show platform hardware qfp active feature bfd datapath sdwan ld 20008
LD                    : 20008
My Private IP         : 172.16.1.1
Remote Private IP     : 192.168.4.0
Tx Stats              : 183600
Rx Stats              : 182912
Encap Type            : IPSEC
State                 : Up
AppProbe              : YES
IPSec Out SA ID       : 0x24000024
Tunnel Rec ID         : 8
IfName                : GigabitEthernet3 (0xf810007f)
Uidb                  : 65528
Config Tx Timer       : 1000000
Conig Detect Timer    : 7000000
Actual Tx Timer       : 1000000
Actual Detect Timer   : 7000000
My Pub IP             : 172.16.1.0
My Pub Port           : 12346
My Symmetric NAT IP   : 0.0.0.0
My Symmetric NAT Port : 0
Remote public IP      : 192.168.4.0
Remote public Port    : 12346
MTU(config), Actual   : 1442, 1442
Farend PMTU           : 1442
My Capabilities       : 0x160
Remote Capabilities   : 0x160
SDWAN BFD flags       : ||||||| (0x0)
local_color           : 4
Ipsec Overhead        : 38
PFR stats for SLA default (addr:0xf14c02a0)
Number of pkts  : 524
```

```
Loss Count      : 0
Latency(1/16ms) : 416
Jitter(1/16ms)  : 832
Following are SDWAN stats
Echo Tx         : 182005
req          : 91415
reply        : 90590
Echo Rx         : 181317
req          : 90590
reply        : 90727
PMTU Tx         : 1595
PMTU RX         : 1595
AppProbeIDValid  NextProbeID StatAddr #Packets  Loss Latency(1/16ms) Jitter(1/16ms)
1         N         0        f14c02c0    0       0       0             0
2         N         0        f14c02e0    0       0       0             0
3         N         0        f14c0300    0       0       0             0
4         N         0        f14c0320    0       0       0             0
5         N         0        f14c0340    0       0       0             0
6         N         0        f14c0360    0       0       0             0
```

show platform hardware qfp active feature firewall drop

To view the drop counters and drop reasons for a firewall, use the **show platform hardware qfp active feature firewall drop** command in user EXEC or privileged EXEC mode.

show platform hardware qfp active feature firewall drop

Command Default

None

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

The following sample output displays the drop reasons.

```
Device# show platform hardware qfp active feature firewall drop

-------------------------------------------------------------------------------
Drop Reason                                                             Packets
-------------------------------------------------------------------------------
ICMP ERR Pkt:exceed burst lmt                                               42
ICMP Unreach pkt exceeds lmt                                               305
UDP - Half-open session limit exceed                                         2
```

show platform hardware qfp active feature geo client

To display the hardware information used for a Cisco Quantum Flow Processor (QFP) to troubleshoot the geo client database, use the **show platform hardware qfp active feature geo client** command in privileged EXEC mode.

show platform hardware qfp active feature geo client { **country** { **all** | **code** *country-code* } | **info** | **stats** }

Syntax Description

country	Displays geo client country information.
all	Displays all the geo client country and continent codes.
code *country-code*	Displays the three-letter country code.
info	Displays information about the control plane policing (CoPP) geo client.
stats	Displays if the geodatabase is enabled or disabled, including updates and errors for troubleshooting.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

The reference counter keeps track of how many IP address table entries belong to the specified country.

Examples

The following are example outputs from the **show platform hardware qfp active feature geo client** command:

```
Device# show platform hardware qfp active feature geo client country all
Country code  ISO-3 code  Country name     Continent code   Continent name   Ref count
-------------------------------------------------------------------------------------
0             ?           unknown          0                **               0
4             afg         afghanistan      4                as               524
8             alb         albania          5                eu               295
```

```
Device# show platform hardware qfp active feature geo client info

Geo DB enabled

DB in use
    File name: /usr/binos/conf/geo_ipv4_db
    Number of entries installed: 415278
    Version: 2134.ajkdbnakjsdn
    Datapath PPE Address: 0x00000000ef2b7010
    Size (bytes): 6644448
    Exmem Handle: 0x0083800109080003
```

```
Country table
    Datapath PPE Address: 0x00000000ef0cf000
    Size (bytes): 16000
    Exmem Handle: 0x0081980009080003
```

The **1** for **Enable received** indicates that the geodatabase has been enabled on the device.

```
Device# show platform hardware qfp active feature geo client stats
CPP client Geo DB stats
-----------------------
  Enable received           : 1
  Modify received           : 0
  Disable received          : 0
  Enable failed             : 0
  Modify failed             : 0
  Disable failed            : 0
  IPv4 table write failed   : 0
  Persona write failed      : 0
  Country table write failed : 0
```

show platform hardware qfp active feature geo datapath

To display information about the hardware used on a Cisco Quantum Flow Processor (QFP) for troubleshooting geo datapath issues, use the **show platform hardware qfp active feature geo datapath** command in privileged EXEC mode.

show platform hardware qfp active feature geo datapath { **country** { **alpha** *alpha-country-code* | **numeric** *numeric-country-code* } | **ip_table** *ip-address* | **memory** | **stats** }

Syntax Description

country	Displays geo client country information.
alpha *alpha-country-code*	Displays the alphabetic country code.
numeric *numeric-country-code*	Displays the numeric country code. Valid values are 1 to 1000.
ip_table *ip-address*	Displays the content of the IP address database.
memory	Displays memory information in the available tables.
stats	Tracks the IP address table lookup results.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

The datapath uses the geodatabase to map IP addresses to geo codes. Geo codes are used for TCAM (ternary content-addressable memory) lookup and classification of data packets.

Examples

The following are example outputs for the **show platform hardware qfp active feature geo datapath** command:

```
Device# show platform hardware qf active feature geo datapath country alpha fra
Country alpha code: fra
Country numeric code: 250
GEO country info:
Country alpha code: fra
Continent alpha code: eu
Continent numeric code: 5
Country ref count: 0
Country hit count: 1
```

```
Device# show platform hardware qfp active feature geo datapath memory
Table-Name   Address      Size
----------------------------------------
Country DB   0xe83a8890   1000
IPV4 DB      0xe9a794a0   415278
```

```
Device# show platform hardware qfp active feature geo datapath stats
GEO Stats:
        lookup hit: 14611371
        lookup miss: 0
        error ip table: 0
        error country table: 0
        country table hit: 14611371
        country table miss: 0
```

show platform hardware qfp active feature nat datapath hsl

To display information about Network Address Translation (NAT) datapath High-Speed Logging (HSL), use the **show platform hardware qfp active feature nat datapath hsl** command in privileged EXEC mode.

show platform hardware qfp active feature nat datapath hsl

Syntax Description

This command has no arguments or keywords.

Command Default

Information about NAT datapath HSL is not displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This command was introduced.
Cisco IOS XE Release 17.6.4 and later 17.6.x releases	

Usage Guidelines

The **show platform hardware qfp active feature nat datapath hsl** command provides information about NAT HSL-specific configurations and enables you to do the following:

- Allows you to troubleshoot NAT issues
- Allows you to verify the feature configurations

Examples

The following is a sample output from the **show platform hardware qfp active feature nat datapath hsl** command that is used to verify the configuration:

```
Device# show platform hardware qfp active feature nat datapath hsl
HSL cfg dip 10.10.0.1 dport 1020 sip 10.21.0.16 sport 53738 vrf 0
nat hsl handle 0x3d007d template id 261 pool_exh template id 263
LOG_TRANS_ADD 132148
LOG_TRANS_DEL 132120
LOG_POOL_EXH 0
```

The following table describes the significant fields shown in the display.

Table 97: show platform hardware Field Descriptions

Field	Description
dip	Destination IP address
dport	Destination port address
sip	Source IP address
sport	Source port address
vrf	VRF ID
LOG_TRANS_ADD	NAT translation added log
LOG_TRANS_DEL	NAT translation deleted log
LOG_POOL_EXH	Pool exhaustion log. NAT also sends an HSL message when a NAT pool runs out of addresses (also called pool exhaustion).

show platform hardware qfp active feature nat datapath map

To display information about NAT mapping tables, use the **show platform hardware qfp active feature nat datapath map** command in privileged EXEC mode.

show platform hardware qfp active feature nat datapath map

Syntax Description

This command has no arguments or keywords.

Command Default

Information about NAT mapping tables is not displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	This command is supported for Cisco Catalyst SD-WAN.

Examples

The following is a sample output from the **show platform hardware qfp active feature nat datapath map** command:

```
Device# show platform hardware qfp active feature nat datapath map
I/f Map Table

if_handle 65529 next 0x0 hash_index 220
laddr 0.0.0.0 lport 0 map 0xdec942c0 refcnt 0
gaddr 200.60.10.1 gport 0 proto 0 vrfid 0x0
src_type 1 flags 0x80100 cpmapid 3
I/f Map Table End
edm maps 0
mapping id 1 pool_id 0 if_handle 0xfff9 match_type 0 source_type 1 domain 0 proto 0 Local
IP 0.0.0.0, Local Port 0 Global IP 200.60.10.1
Global Port 0 Flags 0x80100 refcount 0 cp_mapping_id 3 next 0x0 hashidx 50 vrfid 0 vrf_tableid
 0x0 rg 0 pap_enabled 0 egress_ifh 0x14
```

show platform hardware qfp active feature nat datapath sess-dump

To display a session's summary from the NAT database, use the **show platform hardware qfp active feature nat datapath sess-dump** command in privileged EXEC mode.

show platform hardware qfp active feature nat datapath sess-dump

Syntax Description

This command has no arguments or keywords.

Command Default

Session summary information for the NAT database is not displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	This command is supported for Cisco Catalyst SD-WAN.

Examples

The following is a sample output from the **show platform hardware qfp active feature nat datapath sess-dump** command:

```
Device# show platform hardware qfp active feature nat datapath sess-dump
id 0xdd70c1d0 io 10.20.24.150 oo 10.20.25.150 io 5201 oo 5201 it 200.60.10.1 ot 10.20.25.150
 it 5201 ot 5201 pro 6 vrf 4 tableid
4 bck 65195 in_if 0 out_if 20 ext_flags 0x1 in_pkts 183466
in_bytes 264182128 out_pkts 91731 out_bytes 2987880flowdb in2out fh 0x0 flowdb out2in fh
0x0
id 0xdd70c090 io 10.20.24.150 oo 10.20.25.150 io 25965 oo 25965 it 200.60.10.1 ot 10.20.25.150
 it 25965 ot 25965
pro 1 vrf 4 tableid 4 bck 81393 in_if 0 out_if 20 ext_flags 0x1 in_pkts 27 in_bytes 38610
out_pkts 27
out_bytes 38610flowdb in2out fh 0x0 flowdb out2in fh 0x0
```

show platform hardware qfp active feature nat datapath stats

To display information about NAT datapath statistics, use the **show platform hardware qfp active feature nat datapath stats** command in privileged EXEC mode.

show platform hardware qfp active feature nat datapath stats

Syntax Description This command has no arguments or keywords.

Command Default Information about NAT datapath statistics is not displayed.

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	This command is supported for Cisco Catalyst SD-WAN.

Examples The following is a sample output from the **show platform hardware qfp active feature nat datapath stats** command:

```
Device# show platform hardware qfp active feature nat datapath stats
non_extended 0 entry_timeouts 0 statics 0 static net 0 hits 0 flowdb_hits 0 misses 0
nat_rx_pkts 346062 nat_tx_pkts 666522 nat_unmarked_pkts 0
nat_stick_rx_pkts 0 nat_stick_i2o_pkts 0 nat_stick_o2i_pkts 0
nat_res_port_in2out 0 nat_res_port_out2in 0
non_natted_in2out 0 nat_bypass 0 non_natted_out2in 0
ipv4_nat_stick_forus_hits_pkts 0 ipv4_nat_stick_hit_sb 0
ipv4_nat_stick_ha_ar_pkts 0 ipv4_nat_stick_ha_tcp_fin 0 ipv4_nat_stick_failed_ha_pkts 0
ipv4_nat_alg_bind_pkts 0
Proxy stats:
 ipc_retry_fail 0 cfg_rcvd 12 cfg_rsp 17

Number of sess 0 udp 0 tcp 0 icmp 0
```

show platform hardware qfp active feature nat datapath summary

To display configured and operational data specific to NAT, use the **show platform hardware qfp active feature nat datapath summary** command in privileged EXEC mode.

show platform hardware qfp active feature nat datapath summary

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	This command was introduced.

Usage Guidelines

The **show platform hardware qfp active feature nat datapath summary** command summarizes the following information:

- NAT-specific configurations and statistics
- Allows you to troubleshoot NAT issues
- Provides an overview of features configured

Example

The following is a sample output from the **show platform hardware qfp active feature nat datapath summary** command.

```
Device# show platform hardware qfp active feature nat datapath summary

Nat setting mode: sdwan-default
Number of pools configured: 1
Timeouts: 0(tcp), 0(udp), 0(icmp), 60(dns),
60(syn), 60(finrst), 86400(pptp), 3600(rmap-entry)
pool watermark: not configured
Nat active mapping inside:0 outside:0 static:2 static network:0
Nat datapath debug: enabled
Nat synchronization: enabled
Nat bpa: not configured; pap: not configured
Nat gatekeeper: on
Nat limit configured: no
Vpns configured with match-in-vrf: yes
Nat packet drop: none
Total active translations: 4 (2 static, 2 dynamic, 2 extended)
Platform specific maximum translations: 131072 configured: none
```

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

Table 98: show platform hardware qfp active feature nat datapath summary Field Descriptions

Fields	Description
NAT setting mode	Configures NAT mode to default or cgn or sdwan-default.
Number of pools configured	Configures number of pools for NAT.
Timeouts	Specifies the timeout value that applies to DNS connections (default is 60 secs), ICMP flows (default is 60 secs), TCP port (default is 86400 secs), UDP port (default is 300 secs), synchronous (SYN) timeout value (default is 60 secs), finish and reset timeout value (default is 60 secs), Point-to-Point Tunneling Protocol (PPTP) timeout (default is 86400 secs), Route map entry timeout value (default is 3600 secs).
pool watermark	Generates alerts before addresses in an address pool and are exhausted based on watermark settings.
NAT active mapping	Specifies the statistics of different (inside, outside, static, static network) NAT rules configured.

Fields	Description
NAT debug	Enables debug logging in NAT.
NAT synchronization	Enables NAT synchronization between redundant devices.
NAT bpa	The bulk logging and port block allocation feature allocates a block of port for translation; supported for cgn mode only.
NAT gatekeepers	Optimizes non-natted flows from using excessive CPU usage.
NAT limit configured	The rate limiting NAT translation feature provides you more control over how NAT addresses are used.
VPNs configured with match-in-vrf	Enables inside and outside traffic in the same VRF.
NAT packet drop	Determines if NAT has dropped any packet. Displays true or none.
Total active translations	Displays total number of active IPv4 NAT translations.
Platform specific maximum translations	Configures maximum number of supported IP NAT translations that are specific to the platform.

show platform hardware qfp active feature nat66 datapath prefix

To verify the passed interface stateless NAT66 prefix configuration, use the **show platform hardware qfp active feature nat66 datapath prefix** command in privileged EXEC mode.

show platform hardware qfp active feature nat66 datapath prefix

Syntax Description

This command has no arguments or keywords.

Command Default

No NAT66-configured prefixes are displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command is supported for Cisco Catalyst SD-WAN.

Examples

The following is a sample output from the **show platform hardware qfp active feature nat66 datapath prefix** command:

```
Device# show platform hardware qfp active feature nat66 datapath prefix
prefix hasht 0x89628400 max 2048 chunk 0x8c392bb0 hash_salt 719885386
```

```
NAT66 hash[1] id(1) len(64) vrf(0) in: 2001:db8:ab01:0000:0000:0000:0000:0000 out:
2001:db8:ab02:0000:0000:0000:0000:0000 in2out: 7 out2in: 7
```

show platform hardware qfp active feature nat66 datapath statistics

To verify the global NAT66 statistics, use the **show platform hardware qfp active feature nat66 datapath statistics** command in privileged EXEC mode.

show platform hardware qfp active feature nat66 datapath statistics

Syntax Description

This command has no arguments or keywords.

Command Default

No NAT66 global statistics are displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command is supported for Cisco Catalyst SD-WAN.

Examples

The following is a sample output from the **show platform hardware qfp active feature nat66 datapath statistics** command:

```
Device# show platform hardware qfp active feature nat66 datapath statistics
in2out xlated pkts 7
out2in xlated pkts 7
NAT66_DROP_SC_INVALID_PKT 0
NAT66_DROP_SC_BAD_DGLEN 0
NAT66_DROP_SC_PLU_FAIL 22786
NAT66_DROP_SC_PROCESS_V6_ERR 0
NAT66_DROP_SC_INVALID_EMBEDDED 0
NAT66_DROP_SC_SRC_RT 0
NAT66_DROP_SC_NOT_ENABLED 0
NAT66_DROP_SC_NO_GPM 0
NAT66_DROP_SC_LOOP 0
in2out_pkts 22768 out2in_pkts 22793
in2out_pkts_untrans 22761 out2in_pkts_untrans 22786
in2out_lookup_pass 7 out2in_lookup_pass 7
in2out_lookup_fail 0 out2in_lookup_fail 22786
mem_alloc_fail 0 prefix_fail 0
total prefix count 1
```

show platform hardware qfp active feature sdwan client phy-wan-bind-list

To display the list of interfaces bound to the Physical WAN interface, use the **show platform hardware qfp active feature sdwan client phy-wan-bind-list** command in user EXEC mode.

show platform hardware qfp active feature sdwan client phy-wan-bind-list

Command Default None

Command Modes User EXEC (>)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	This command was introduced.

Examples The following sample output displays the list of interfaces bound to the Physical WAN interface.

```
Device# show platform hardware qfp active feature sdwan client phy-wan-bind-list
physical interface(if_hdl)------------bind interfaces(if_hdl)

GigabitEthernet0/0/0(7)               GigabitEthernet0/0/0(7)
```

show platform hardware qfp active feature utd config

To verify the UTD data plane configuration, use the **show platform hardware qfp active feature utd config** command in privileged EXEC mode.

show platform hardware qfp active feature utd config

Command Default None

Command Modes Privileged EXEC (#)

Command History

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

Usage Guidelines Use this command to display UTD datapath configuration and status.

Example

The following example shows the UTD datapath configuration and status.

```
Device# show platform hardware qfp active feature utd config
Global configuration
  NAT64: disabled
  Drop pkts: disabled
  Multi-tenancy: disabled
  Data plane initialized: yes
  TLS Decryption Policy: disabled
```

```
Divert controller mode: enabled
SN threads: 12
CFT inst_id 0 feat id 4 fo id 4 chunk id 17
Max flows: 55000
```

Note There is a maximum number of flows supported by UTD, and you can use the **show platform hardware qfp active feature utd config** command to identify the maximum number of concurrent sessions supported on a Cisco IOS XE Catalyst SD-WAN device. Max flows are defined for each Cisco IOS XE Catalyst SD-WAN device, and it differs by devices and release versions. This example displays a Max Flow value defined for 55000 sessions.

show platform hardware qfp active interface if-name

To display packet drop statistics for each interface in the Quantum Flow Processor (QFP), use the **show platform hardware qfp active interface if-name** command in privileged EXEC mode.

show platform hardware qfp active interface if-name *type number* **statistics** [**clear_drop** | **detail** | **drop_summary** [**subinterface**]]

Syntax Description

type	Interface Type.
number	Interface Number.
statistics	Tx/Rx and Drop statistics.
clear_drop	(Optional) Clears drop stats after reading.
detail	(Optional) Shows drop cause IDs.
drop_summary	(Optional) Drops stats summary report.
subinterface	(Optional) Shows subinterface and their drop stats.

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines Use this command for troubleshooting an interface in a QFP by analyzing the statistics of packet drops.

Example

The following example shows how to display the statistics of packet drops on the Gigabit Ethernet interface 0/0/0.

```
Device# show platform hardware qfp active interface if-name gigabitEthernet 0/0/0 statistics
------------------------------------------------------------------
Receive Stats Packets Octets
------------------------------------------------------------------
Ipv4 2 322
Ipv6 0 0
Tag 0 0
McastIpv4 0 0
McastIpv6 0 0
Other 3 204
------------------------------------------------------------------
Transmit Stats Packets Octets
------------------------------------------------------------------
Ipv4 2 178
Ipv6 0 0
Tag 0 0
McastIpv4 0 0
McastIpv6 0 0
Other 0 0
------------------------------------------------------------------
Input Drop Stats Packets Octets
------------------------------------------------------------------
Ipv4uRpfStrictFailed 5 590
Ipv6uRpfStrictFailed 5 590
------------------------------------------------------------------
Output Drop Stats Packets Octets
------------------------------------------------------------------
The Egress drop stats were all zero
------------------------------------------------------------------
Drop Stats Summary:
note: 1) these drop stats are only updated when PAL
reads the interface stats.
2) the interface stats include the subinterface
Interface Rx Pkts Tx Pkts
------------------------------------------------------------------------------
GigabitEthernet0/0/0 25 0
```

show platform hardware qfp active statistics drop

To display the drop statistics for all interfaces, use the **show platform hardware qfp active statistics drop** command in user EXEC mode.

show platform hardware qfp active statistics drop

Command Default None

Command Modes User EXEC (>)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	This command was introduced.

Examples

The following sample output displays the drop statistics for all interfaces.

```
Device# show platform hardware qfp active statistics drop
Last clearing of QFP drops statistics : never


-----------------------------------------------------------------------
Global Drop Stats                          Packets                Octets
-----------------------------------------------------------------------
Disabled                                         4                   266
Ipv4EgressIntfEnforce                           15                 10968
Ipv6NoRoute                                      6                   336
Nat64v6tov4                                      6                   480
SVIInputInvalidMac                             244                 15886
SdwanImplicitAclDrop                           160                 27163
UnconfiguredIpv4Fia                         942525              58524580
UnconfiguredIpv6Fia                          77521               9587636
```

show platform hardware qfp active feature firewall datapath rg

To display detailed information about the firewall datapath within a redundancy group on a Cisco IOS XE Catalyst SD-WAN device, use the **show platform hardware qfp active feature firewall datapath rg** command in privileged EXEC mode.

show platform hardware qfp active feature firewall datapath rg

Syntax Description

group	Display details of the firewall datapath for a redundancy group.
all	Displays all statistics providing detailed insights into the current state and performance metrics of both the active and standby components of an high availability system.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.15.1a	This command is supported for Cisco Catalyst SD-WAN.

Usage Guidelines

Use the **show platform hardware qfp active feature firewall datapath rg** to display detailed information about the firewall datapath within a redundancy group.

Examples

The following is a sample output from the **show platform hardware qfp active feature firewall datapath rg** command with the redundancy group set to 1.

```
Device# show platform hardware qfp active feature firewall datapath rg 1

rg 1, rg_state 0x00030035 (Active, Transport Up, Flow On, AR Transport UP, Allow New Sessions,
 Update Peer)
11 (RG Active) ha_handle 0x00020102 rg_flags 0x0 session id 0x5

==== HA general stat ====
Initial bulksync retry count 0
Allocated retry entries 0
Current retry queue depth 0
Maximum queued retries 0
Max retries queued ever 0
Stats were all zero

==== HA active stat ====
Total received messages 1
Session create requests 5
Session delete requests 5
Bulksync requests received 1
Bulksync complete 1
Session sync attempt: create 5
Session sync attempt: delete 5

==== HA standby stat ====
Stats were all zero
```

Examples

The following is a sample output from the **show platform hardware qfp active feature firewall datapath rg** command with the redundancy group set to all.

```
Device# show platform hardware qfp active feature firewall datapath rg all

rg 1, rg_state 0x00030035 (Active, Transport Up, Flow On, AR Transport UP, Allow New Sessions,
 Update Peer)
11 (RG Active) ha_handle 0x00020102 rg_flags 0x0 session id 0x5

==== HA general stat ====
Initial bulksync retry count 0
Allocated retry entries 0
Current retry queue depth 0
Maximum queued retries 0
Max retries queued ever 0
Total retry allocations 0
Retry allocation failures 0
Total retry entries queued 0
Flow on 0
Flow off 0
Retry timeout 0

==== HA active stat ====
```

```
Total received messages 1
Missing RII 0
Session create requests 5
Session delete requests 5
Session update requests 0
Bulksync requests received 1
Bulksync complete 1
L7 buffers allocated 0
L7 buf alloc failure 0
Failed to send L7 data 0
L7 data sent 0
Invalid opcode recvd 0
Message too short 0
Bad version number 0
Bad magic number 0
Create NAKs received 0
No HA buffer 0
No buffer false positive 0
Session sync attempt: create 5
Session sync attempt: update 0
Session sync attempt: delete 5
Session sync attempt: l7 data 0
vrf mapping failures 0
Invalid protocol 0
PAM classificaiton failure 0
Classificaiton failure 0
Could not find parent flow 0
Asymmetric routing injection 0
Data transport down 0
Bad bulk sync feature id 0
Bad bulk sync message length 0
Bulk sync error: init not complete 0
Bulk sync - active now standby 0
Bulk sync - Standby not read 0
Transport Down 0
Attempt to initiate bulk sync on active 0
Invalid no response bulk sync timer on active 0
Bulk sync request retry re-queued 0
Bulk sync request retry re-queue failed 0
Bulk sync done re-queued 0
Bulk sync done re-queue failed 0

==== HA standby stat ====
Total received messages 0
Session create requests 0
Session delete requests 0
Session update requests 0
Create NAK sent 0
Inspection policy not found 0
Could not create session 0
Could not create subordinate session 0
New sessions not allowed 0
Could not locate ingress uidb RII 0
Could not locate egress uidb RII 0
RG not configured 0
Could not locate uidb sub-block 0
Invalid zone - no inspection 0
Invalid zone - drop 0
Invalid zone pair 0
Classification failed 0
Classification results missing stats 0
Subflow RG mismatch 0
RG mismatch on create/flow exists 0
Could not find session 0
```

```
Session RG mismatch 0
Session delete miss 0
Session delete RG mismatch 0
Layer 7 data 0
Rcvd bad opcode 0
Msg too short 0
Unsupported msg version 0
Bulk sync requested 0
Bulk sync requested timeout 0
Bulk sync requested failed 0
Bulk Sync msg sent 0
Bulk sync complete 0
Peer not identified 0
Could not allocate msg buffer 0
Could not find VRF 0
Asymmetric routing redirect 0
Asymmetric routing redirect failed - no uidb_sb 0
Asymmetric routing redirect failed - no AR 0
Transport Down 0
Bulk sync failed : no response 0
Existing session removed/replaced 0
Invalid message magic number 0
```

show platform hardware qfp active feature firewall drop all

To display all drop counts, use the **show platform hardware qfp active feature firewall drop all** command in privileged EXEC mode.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	This command is supported in Cisco Catalyst SD-WAN

Example

The following example displays all drop counts,.

```
Device#show platform hardware qfp active feature firewall drop all
-----------------------------------------------------------------------------
Drop Reason                                                          Packets
-----------------------------------------------------------------------------
Invalid L4 header                                                          0
Invalid ACK flag                                                           0
Invalid ACK number                                                         0
Invalid TCP initiator                                                      0
SYN with data                                                              0
Invalid window scale option                                                0
Invalid Segment in SYNSENT                                                 0
Invalid Segment in SYNRCVD                                                 0
TCP out of window                                                          0
TCP window overflow                                                        0
TCP extra payload after FIN                                                0
Invalid TCP flags                                                          0
Invalid sequence number                                                    0
Retrans with invalid flags                                                 0
```

```
TCP out-of-order segment                                                0
SYN flood drop                                                          0
INT ERR:synflood h-tdl alloc fail                                       0
Synflood blackout drop                                                  0
TCP - Half-open session limit exceed                                    0
Too many packet per flow                                                0
ICMP ERR PKT per flow exceeds                                           0
Unexpect TCP pyld in handshake                                          0
INT ERR:Undefined direction                                             0
SYN inside current window                                               0
RST inside current window                                               0
Stray Segment                                                           0
RST sent to responder                                                   0
ICMP INT ERR:Missing NAT info                                           0
ICMP INT ERR:Fail to get ErrPkt                                         0
ICMP INT ERR:Fail to get Statbk                                         0
ICMP INT ERR:direction undefined                                        0
ICMP PKT rcvd in SCB close st                                           0
Missed IP hdr in ICMP packet                                            0
ICMP ERR PKT:no IP or ICMP                                              0
ICMP ERR Pkt:exceed burst lmt                                           0
ICMP Unreach pkt exceeds lmt                                            0
ICMP Error Pkt invalid sequence                                         0
ICMP Error Pkt invalid ACK                                              0
ICMP Error Pkt too short                                                0
Exceed session limit                                                    0
Packet rcvd in SCB close state                                          0
Pkt rcvd after CX req teardown                                          0
CXSC not running                                                        0
Zone-pair without policy                                                0
Same zone without Policy                                                0
ICMP ERR:Policy not present                                             0
Classification Failed                                                   0
Policy drop:non tcp/udp/icmp                                            0
PAM lookup action drop                                                  0
ICMP Error Packet TCAM missed                                           0
Security policy misconfigure                                            0
INT ERR:Get stat blk failed                                             0
IPv6 dest addr lookup failed                                            0
SYN cookie max dst reached                                              0
INT ERR:syncook d-tbl alloc failed                                      0
SYN cookie being triggered                                              0
Fragment drop                                                           0
Policy drop:classify result                                            11
ICMP policy drop:classify result                                        0
L7 segmented packet not allow                                           0
L7 fragmented packet not allow                                          0
L7 unknown proto type                                                   0
L7 inspection returns drop                                              0
Promote fail due to no zone pair                                        0
Promote fail due to no policy                                           0
Firewall Create Session fail                                            0
Firewall No new session allow                                           0
Not a session initiator                                                 0
Firewall invalid zone                                                  18
Firewall AR standby                                                     0
Firewall no forwarding allow                                            0
Firewall back pressure                                                  0
Firewall LISP hdr restore fail                                          0
Firewall LISP inner pkt insane                                          0
Firewall LISP inner ipv4 insane                                         0
Firewall LISP inner ipv6 insane                                         0
Firewall zone check failed                                              0
Could not register flow with FBD                                        0
```

```
Invalid drop event                                                      0
Invalid drop event                                                      0
Invalid drop event                                                      0
Invalid ICMP sequence number                                            0
UDP - Half-open session limit exceed                                    0
ICMP - Half-open session limit exceed                                   0
AVC Policy drop:classify result                                         0
Could not aquire session lock                                           0
No Zone-pair found                                                      0
```

show platform hardware qfp active feature bridge-domain datapath sdwan-flood-list

To display information about flood list of a bridge domain in the data plane, use the **show platform hardware qfp active feature bridge-domain datapath sdwan-flood-list** command in privileged EXEC (#).

show platform hardware qfp active feature bridge-domain datapath [*bridge-domain-id*] [**sdwan-flood-list**]

Syntax Description

bridge-domain-id	Displays the L2VPN status for a specific L2VPN SDWAN instance. Specify vc-id the value. Range:1 to 65531
sdwan-flood-list	Displays Virtual Circuit (VC) ID that is used to identify a particular bridge domain. Specify vc-id the value. Range:1 to 65531

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.14.1a	This command was introduced.

Examples

The following sample output displays the Cisco SD-WAN flood list for a bridge-domain in data plane:

```
Device# show platform hardware qfp active feature bridge-domain datapath 13 sdwan-flood-list
l2vpn:13 sdwan-olist:0xe0d36d80

Flood List for Bridge Domain 13:
 BDI13
 SDWAN oce_base:0xe1961a40 intf:SFI13.13.4210709 flags:
 SDWAN oce_base:0xe1961680 intf:SFI13.13.4210709 flags:
```

show platform packet-trace

To view detailed packet tracer statistics for a specified trace ID or summary statistics for all the filtered packets, for up to 1024 records, use the **show platform packet-trace** command in privileged EXEC mode.

show platform packet-trace [**details** *trace-id*] [**summary**]

Syntax Description

details *trace-id*	(Optional) Displays packet trace details for the specified trace ID.
summary	(Optional) Displays packet trace statistics for the specified packets.
trace-id	(Optional) Displays packet statistics for the specified trace-id. Range: 0 to 1023.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	This command was introduced.

Example

The following example displays the packet trace summary.

```
Device# show platform packet-trace summary

Pkt   Input                Output               State  Reason
0     INJ.12               Gi2                  FWD
1     Gi2                  internal0/0/rp:0     PUNT   5    (CLNS IS-IS Control)
2     INJ.1                Gi2                  FWD
3     INJ.1                Gi2                  FWD
4     Gi2                  internal0/0/rp:0     PUNT   5    (CLNS IS-IS Control)
5     Gi2                  internal0/0/rp:0     PUNT   5    (CLNS IS-IS Control)
6     INJ.1                Gi2                  FWD
7     INJ.1                Gi2                  FWD
8     Gi2                  internal0/0/rp:0     PUNT   5    (CLNS IS-IS Control)
9     Gi2                  internal0/0/rp:0     PUNT   5    (CLNS IS-IS Control)
10    Gi2                  internal0/0/rp:0     PUNT   5    (CLNS IS-IS Control)
11    INJ.1                Gi2                  FWD
12    Gi2                  internal0/0/rp:0     PUNT   5    (CLNS IS-IS Control)
13    INJ.1                Gi2                  FWD
14    INJ.1                Gi2                  FWD
```

The following is the sample output for the show packet trace details command, which is displayed for the specified trace ID 0.

```
Device# show platform packet-trace packet 0

Packet: 0           CBUG ID: 4321
Summary
  Input     : GigabitEthernet2
  Output    : GigabitEthernet3
  State     : FWD
  Timestamp
    Start   : 1124044721695603 ns (09/20/2022 01:47:28.531049 UTC)
    Stop    : 1124044722142898 ns (09/20/2022 01:47:28.531497 UTC)
Path Trace
  Feature: IPV4(Input)
    Input       : GigabitEthernet2
    Output      : <unknown>
    Source      : 10.10.10.10
    Destination : 20.20.20.20
    Protocol    : 1 (ICMP)
  Feature: DEBUG_COND_INPUT_PKT
    Entry       : Input - 0x814670b0
    Input       : GigabitEthernet2
    Output      : <unknown>
    Lapsed time : 600 ns
  Feature: IPV4_INPUT_DST_LOOKUP_ISSUE
    Entry       : Input - 0x81494d2c
    Input       : GigabitEthernet2
    Output      : <unknown>
    Lapsed time : 1709 ns
  Feature: IPV4_INPUT_ARL_SANITY
    Entry       : Input - 0x814690e0
    Input       : GigabitEthernet2
    Output      : <unknown>
    Lapsed time : 1274 ns
  Feature: IPV4_INPUT_DST_LOOKUP_CONSUME
    Entry       : Input - 0x81494d28
    Input       : GigabitEthernet2
    Output      : <unknown>
    Lapsed time : 269 ns
  Feature: IPV4_INPUT_FOR_US_MARTIAN
    Entry       : Input - 0x81494d34
    Input       : GigabitEthernet2
    Output      : <unknown>
    Lapsed time : 384 ns
  Feature: DEBUG_COND_APPLICATION_IN
    Entry       : Input - 0x814670a0
    Input       : GigabitEthernet2
    Output      : <unknown>
    Lapsed time : 107 ns
  Feature: DEBUG_COND_APPLICATION_IN_CLR_TXT
    Entry       : Input - 0x8146709c
    Input       : GigabitEthernet2
    Output      : <unknown>
    Lapsed time : 36 ns
  Feature: IPV4_INPUT_LOOKUP_PROCESS
    Entry       : Input - 0x81494d40
    Input       : GigabitEthernet2
    Output      : GigabitEthernet3
    Lapsed time : 38331 ns
  Feature: IPV4_INPUT_IPOPTIONS_PROCESS
    Entry       : Input - 0x81495258
    Input       : GigabitEthernet2
    Output      : GigabitEthernet3
    Lapsed time : 259 ns
  Feature: IPV4_INPUT_GOTO_OUTPUT_FEATURE
    Entry       : Input - 0x8146ab58
```

```
    Input       : GigabitEthernet2
    Output      : GigabitEthernet3
    Lapsed time : 9485 ns
  Feature: IPV4_VFR_REFRAG
    Entry       : Output - 0x81495c6c
    Input       : GigabitEthernet2
    Output      : GigabitEthernet3
    Lapsed time : 520 ns
  Feature: IPV6_VFR_REFRAG
    Entry       : Output - 0x81496600
    Input       : GigabitEthernet2
    Output      : GigabitEthernet3
    Lapsed time : 296 ns
  Feature: MPLS(Output)
    Input       : GigabitEthernet2
    Output      : GigabitEthernet3
    Label Stack Entry[1]: 0x03e850fe
      StackEnd:NO, TTL:254, EXP:0, Label:16005, is SDWAN:NO
    Label Stack Entry[2]: 0x000121fe
      StackEnd:YES, TTL:254, EXP:0, Label:18, is SDWAN:NO
  Feature: MPLS_OUTPUT_ADD_LABEL
    Entry       : Output - 0x8145e130
    Input       : GigabitEthernet2
    Output      : GigabitEthernet3
    Lapsed time : 29790 ns
  Feature: MPLS_OUTPUT_L2_REWRITE
    Entry       : Output - 0x812f4724
    Input       : GigabitEthernet2
    Output      : GigabitEthernet3
    Lapsed time : 23041 ns
  Feature: MPLS_OUTPUT_FRAG
    Entry       : Output - 0x8149ae5c
    Input       : GigabitEthernet2
    Output      : GigabitEthernet3
    Lapsed time : 785 ns
  Feature: MPLS_OUTPUT_DROP_POLICY
    Entry       : Output - 0x8149ebdc
    Input       : GigabitEthernet2
    Output      : GigabitEthernet3
    Lapsed time : 14697 ns
  Feature: MARMOT_SPA_D_TRANSMIT_PKT
    Entry       : Output - 0x814ac56c
    Input       : GigabitEthernet2
    Output      : GigabitEthernet3
    Lapsed time : 45662 ns
Packet Copy In
  00505683 d54f0050 56830863 08004500 00641018 0000ff01 6f450a0a 0a0a1414
  14140800 3839001c 00000000 00005b3a eabaabcd abcdabcd abcdabcd abcdabcd
Packet Copy Out
  00505683 d4900050 5683429a 884703e8 50fe0001 21fe4500 00641018 0000fe01
  70450a0a 0a0a1414 14140800 3839001c 00000000 00005b3a eabaabcd abcdabcd
```

show platform packet-trace fia-statistics

To view Feature Invocation Array (FIA) statistics about a feature, use the **show platform packet-trace fia-statistics** command in the privileged EXEC mode.

show platform packet-trace fia-statistics

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	This command was introduced.

Example

The following example displays FIA statistics on Cisco IOS XE Catalyst SD-WAN devices.

```
Device# show platform packet-trace fia-statistics

Feature                                          Count  Min(ns)   Max(ns)   Avg(ns)
-------------------------------------------------------------------------------------
INTERNAL_TRANSMIT_PKT_EXT                           66     4720     28400     13333
MARMOT_SPA_D_TRANSMIT_PKT_EXT                       16     4560     16920     11955
L2_SVI_OUTPUT_BRIDGE_EXT                             1     3640      3640      3640
INTERNAL_INPUT_GOTO_OUTPUT_FEATURE_EXT              16     1680      3880      2755
IPV4_INPUT_LOOKUP_PROCESS_EXT                        1     2720      2720      2720
IPV4_OUTPUT_L2_REWRITE_EXT                           1     2240      2240      2240
IPV4_OUTPUT_DROP_POLICY_EXT                          4     1040      2880      2050
IPV4_INTERNAL_DST_LOOKUP_CONSUME_EXT                 1     1960      1960      1960
SSLVPN_INJECT_TX_MSG_EXT                            15      600      2440      1746
IPV4_INTERNAL_FOR_US_EXT                             1     1560      1560      1560
LAYER2_OUTPUT_QOS_EXT                               63      280      2480      1537
LAYER2_OUTPUT_DROP_POLICY_EXT                       78      120      3120      1525
LAYER2_INPUT_LOOKUP_PROCESS_EXT                     15      280      2240      1312
UPDATE_ICMP_PKT_EXT                                  1     1280      1280      1280
DEBUG_COND_MAC_EGRESS_EXT                            3      840      1160       973
IPV4_INTERNAL_INPUT_SRC_LOOKUP_CONSUME_EXT           1      960       960       960
IPV4_PREF_TX_IF_SELECT_EXT                           1      800       800       800
DEBUG_COND_OUTPUT_PKT_EXT                           66       80      1640       707
IPV4_INTERNAL_ARL_SANITY_EXT                         3      240       960       666
IPV4_INTERNAL_INPUT_SRC_LOOKUP_ISSUE_EXT             1      640       640       640
IPV4_VFR_REFRAG_EXT                                  5      320       920       640
EVC_EFP_VLAN_TAG_ATTACH_EXT                         15       80      1040       629
L2_SVI_OUTPUT_GOTO_OUTPUT_FEATURE_EXT                1      520       520       520
LAYER2_VLAN_INJECT_EXT                              15      120       760       504
L2_ES_OUTPUT_PRE_TX_EXT                             16        0      1000       502
DEBUG_COND_APPLICATION_IN_EXT                        1      480       480       480
DEBUG_COND_APPLICATION_OUT_CLR_TXT_EXT               3       80       720       426
DEBUG_COND_INPUT_PKT_EXT                            16       80       880       417
IPV4_OUTPUT_FRAG_EXT                                 1      360       360       360
DEBUG_COND_APPLICATION_IN_CLR_TXT_EXT                1      320       320       320
DEBUG_COND_APPLICATION_OUT_EXT                       3      240       280       266
LFTS_INJECT_PKT_EXT                                 16       40       480       250
LAYER2_BRIDGE_INJECT_EXT                            15       40       560       234
```

show platform software common-classification f0 tag

To display the tag information from forwarding manager on forwarding plane (FMAN-FP), use the **show platform software common-classification f0 tag** command in privileged EXEC mode.

show platform software common-classification f0 tag { *all* | *tag-id* { **app-list** | **prefix-list** | **sets** | **summary** } }

Syntax Description

f0	Embedded-Service-Processor slot 0.
all	All tags.
id	Tag ID. Range: 1 to 4294967295.
summary	Displays the summary information for one particular tag-instance. Based on this show output, user can further display prefix-list or app-list or sets for this tag-instance.
prefix-list	Prefix list type members.
app-list	App ID list type members.
sets	Tag rule sets.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This command was introduced.

Usage Guidelines

The **show platform software common-classification fo tag** command is used for troubleshooting purposes.

Examples

The following is a sample output from the **show platform software common-classification fo tag** command displaying the tag information from a forwarding manager on a forwarding plane (FMAN-FP):

```
Device# show platform software common-classification F0 tag all
Total Number of TAGs: 9
tag id       tag name              tag type     num clients  num sets     num member types
  total members
-------------------------------------------------------------------------------------------------
900          special_TAG7          Per Type OR  0            2            1
  2
10000        DP_V4_TAG1            Per Type OR  1            1            1
  1
11000        DP_V4_TAG2            Per Type OR  1            2            1
  2
12000        DP_V4_TAG3            Per Type OR  1            6            1
  6
20000        DP_V6_TAG4            Per Type OR  1            1            1
  1
21000        DP_V6_TAG5            Per Type OR  1            2            1
  2
50000        APP_webex_TAG8        Per Type OR  1            1            1
  1
60000        APP_facebook_TAG9     Per Type OR  1            1            1
  1
70000        APP_office_TAG10      Per Type OR  1            2            1
  2

Device# show platform software common-classification f0 tag 1 summary
TAG ID: 1
TAG TYPE: Per Type OR
```

```
TAG Name: net1
Is Dummy: F

client data:
  client id     client name
  ---------------------------------
  166           SDWAN

member data:
  Prefix List           6
  App List              3
```

```
Device# show platform software common-classification f0 tag 1 prefixList
 member details:
  member detail type    member id     member data
  ------------------------------------------------
  IPv4 Prefix List      65537         100
  IPv6 Prefix List      65538         101
  IPv4 Prefix List      65540         103
  IPv6 Prefix List      65541         104
  IPv6 Prefix List      65544         107
  IPv4 Prefix List      65546         109
```

```
Device# show platform software common-classification f0 tag 1 appList
 member details:
  member detail type    member id     member data
  ------------------------------------------------
  App List              65539         102
  App List              65542         105
  App List              65545         108
```

```
Device# show platform software common-classification f0 tag 1 set
Total Number of SETs: 18
  Set ID        member detail type    member id     member data
  ------------------------------------------------------------
  1             IPv4 Prefix List      65537         100
  1             App List              65539         102
  2             IPv4 Prefix List      65537         100
  2             App List              65542         105
  3             IPv4 Prefix List      65537         100
  3             App List              65545         108
  4             IPv6 Prefix List      65538         101
  4             App List              65539         102
  5             IPv6 Prefix List      65538         101
```

show platform software cpu alloc

To view the CPU cores allocated on a device, use the **show platform software cpu alloc** command in privileged EXEC mode.

show platform software cpu alloc

Command Modes

privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	This command was introduced.

Example

Following is the sample output from the **show platform software cpu alloc** command and shows the core allocation on a Cisco Catalyst 8000V instance with six cores:

```
Device# show platform software cpu alloc

CPU alloc information:


  Control plane cpu alloc: 0


  Data plane cpu alloc: 4-5


  Service plane cpu alloc: 1-3


  Template used: CLI-service_plane_heavy
```

This example shows the core allocation on a Cisco Catalyst 8000V instance with eight cores:

```
Device# show platform software cpu alloc

CPU alloc information:


  Control plane cpu alloc: 0


  Data plane cpu alloc: 6-7


  Service plane cpu alloc: 1-5


  Template used: CLI-service_plane_heavy
```

This example shows the core allocation on a Cisco Catalyst 8000V instance with 12 cores:

```
Device# show platform software cpu alloc

CPU alloc information:


  Control plane cpu alloc: 0


  Data plane cpu alloc: 9-11


  Service plane cpu alloc: 1-8
```

```
  Template used: CLI-service_plane_heavy
```

This example shows the core allocation on a Cisco Catalyst 8000V instance with 16 cores:

```
Device# show platform software cpu alloc

CPU alloc information:


  Control plane cpu alloc: 0


  Data plane cpu alloc: 12-15


  Service plane cpu alloc: 1-11


  Template used: CLI-service_plane_heavy
```

show platform software ipsec fp active flow

To display information about active instances of IPsec flows, use the **show platform software fp ipsec active flow** command in privileged EXEC mode.

show platform software ipsec fp active flow { **all** | **identifier** *number* }

Syntax Description

all	Displays information about all active IPsec flows in the instance.
identifier *number*	Displays information about the specified IPsec flow in the instance. Range: 0 - 4294967295

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.15.1a	This command is supported in Cisco Catalyst SD-WAN. Starting from Cisco IOS XE Catalyst SD-WAN Release 17.15.1a, the output of this command was modified with an increased flow ID range. Range: 0 - 4294967295

Usage Guidelines

For usage guidelines, see the Cisco IOS XE show platform software ipsec fp active flow command.

The following is sample output from the **show platform software ipsec fp active flow** command for flow ID 2146:

```
Device# show platform software ipsec fp active flow identifier 2146
========== Flow id: 2146
              mode: transport
         direction: outbound
          protocol: esp
               SPI: 0x000102
     local IP addr: 213.103.103.0
    remote IP addr: 170.132.2.2
  crypto device id: 0
     crypto map id: 1043
            SPD id: 3
        QFP SPD id: 3
   ACE line number: 1
     QFP SA handle: 3024
   QFP SA PPE addr: 0x83af0210
IOS XE interface id: 56
     interface name: Tunnel2
       use path MTU: 1480
  Crypto SA ctx id: 0x000000006d01f7aa
            cipher: AES-256 GCM (AAD with AH-NO-ID)
              auth: null
 initial seq.number: 0
      timeout, mins: 0
              flags: exp time;exp traffic;NAT-T;NAT orig address;
Time limits

    soft limit(sec): 0
    hard limit(sec): 809108523
Traffic limits

     soft limit(kB): 0
     hard limit(kB): 17448352331316854784
no expiry sent

     total soft expiry notification: 0
     total hard expiry notification: 0
     total rekey request received: 0
     total rekey request updated : 0
     total rekey request skipped : 0
-- NAT-T

     local UDP port: 12346
    remote UDP port: 12346
    original IP addr: 170.132.2.2
     inline_tagging: DISABLED
 ext_ar_window_size: 0
Classifier: range

   src IP addr low: 213.103.103.0
  src IP addr high: 213.103.103.0
   dst IP addr low: 170.132.2.2
  dst IP addr high: 170.132.2.2
      src port low: 12346
     src port high: 12346
      dst port low: 12346
     dst port high: 12346
      protocol low: 0
     protocol high: 255
------------- Statistics

            octets(delta): 0
```

```
      total octets(delta): 10664523917613334528
           packets(delta): 106058
   dropped packets(delta): 0
      replay drops(delta): 0
      auth packets(delta): 0
        auth fails(delta): 0
 encrypted packets(delta): 106058
     encrypt fails(delta): 0
---------- End statistics

       object state: active
  object bind state: active
--------------- AOM

         cpp aom id: 28463
         cgm aom id: 28462
          n2 aom id: 28459
          if aom id: 0
```

The following table describes the significant fields shown in the display.

Table 99: show platform software ipsec fp active flow identifier Field Descriptions

Field	Description
Flow id	Flow identifier.
mode	Operation mode. In this case, it is tunnel mode.
direction	Flow direction—inbound or outbound. In this case, it is outbound.
protocol	Protocol used. In this case, it is Encapsulating Security Payloads (ESP).
SPI	Security Parameters Index (SPI) that is used to identify the security association (SA).
local IP addr	IP address of the local host.
remote IP addr	IP address of the remote host.
crypto map id	Crypto map identifier.
SPD id	SPI identifier.
ACE line number	Cisco Application Control Engine (ACE) number.
QFP SA handle	Quantum Flow Processor (QFP) SA identifier.
crypto device id	Crypto device identifier.
IOS XE interface id	Interface ID in Cisco IOS XE software.
interface name	Interface name.
Crypto SA ctx id	Context identifier of the crypto SA.
cipher	Type of encryption algorithm.
auth	Type of authentication algorithm.

Field	Description
initial seq.number	Initial sequence number.
timeout, mins	Timeout, in minutes.
flags	Flags set for the packet flow.
Peer Flow handle	Peer flow identifier.
Time limits soft limit	Minimum permissible time limit.
Time limits hard limit	Maximum permissible time limit.
Traffic limits soft limit	Minimum permissible traffic limit.
Traffic limits hard limit	Maximum permissible traffic limit.
DPD	Dead peer detection (DPD).
mode	DPD mode. In this case, it is periodic.
rearm countdown	Rearm for DPD.
next notify	Status of next notification.
last in packet	Status of the last packet.
inline_tagging	Status of inline tagging.
anti-replay window	Status of anti-replay window.
SPI Selector	Information about SPI selection.
remote addr low	Starting range address of the remote host.
remote addr high	Highest range address of the remote host.
local addr low	Starting range address of the local host.
local addr high	Highest range address of the local host.
Classifier	Type of classification.
src IP addr low	Starting range of the source IP address.
src IP addr high	Highest range of the source IP address.
dst IP addr low	Starting range of the destination IP address.
dst IP addr high	Highest range of the destination IP address.
src port low	Starting range of the source port.
src port high	Highest range of the source port.
dst port low	Starting range of the destination port.

Field	Description
dst port high	Highest range of the destination port.
protocol low	Starting range of the protocol.
protocol high	Highest range of the protocol.
octets	Number of octets in the packet.
total octets	Total number of octets.
packets	Number of packets.
dropped packets	Number of packets dropped.
replay drops	Number of packets that were dropped again.
auth packets	Number of packets authenticated.
auth fails	Number of packets for which authentication failed.
encrypted packets	Number of encrypted packets.
encrypt fails	Number of packets for which encryption failed.
object state	Object state. In this case, it is active.
cpp aom id	Cisco Packet Processor Asynchronous Object Manager (AOM) identifier.
cgm aom id	Class Group Manager AOM identifier.
n2 aom id	Cavium NITROX II cryptographic coprocessor AOM identifier.
if aom id	Interface AOM identifier.

show platform software ipsec ftm-msg-stats

To displays message exchange statistics between SDWAN-RP and the IPSec module, use the **show platform software ipsec ftm-msg-stats** command in privileged EXEC mode.

show platform software ipsec ftm-msg-stats

Syntax Description

This command has no keywords or arguments.

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.14.1a	This command was introduced.

Usage Guidelines

Use these commands only on Cisco IOS XE Catalyst SD-WAN devices.

The following is a sample output that shows the message exchange statistics between SDWAN-RP and the IPSec module:

```
Device# show platform software ipsec ftm-msg-stats
MSG Type    From SDWAN    Suppressed         OK         ERR
             DELETE             0             0           0           0
             UPDATE           506             0         506           0

             MSG Type      To VESEN    Suppressed         OK         ERR
             CREATE             506             0         506           0
             DELETE               0             0           0           0
             UPDATE               0             0           0           0
          REKEY(IN)               0             0           0           0
         REKEY(OUT)               0             0           0           0

            Ring Name       Read     Write    ReadERR   WriteERR ItemCount
            DCR Ring           0         0          0          0         0
            DDM Ring           0         0          0          0         0
```

show platform software ipsec sdwanrp-msg-stats

To displays message exchange statistics between SDWAN-RP and the IPSec module, use the **show platform software ipsec sdwanrp-msg-stats** command in privileged EXEC mode.

show platform software ipsec sdwanrp-msg-stats

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 26.1.1	This command was introduced.

Usage Guidelines

Use these commands only on Cisco IOS XE Catalyst SD-WAN devices.

The following is a sample output that shows the message exchange statistics between SDWAN-RP and the IPSec module:

```
Device# show platform software ipsec sdwanrp-msg-stats
MSG Type    From SDWAN   Suppressed        OK        ERR
             DELETE            0            0          0          0
             UPDATE          506            0        506          0

             MSG Type     To VESEN   Suppressed        OK        ERR
             CREATE          506            0        506          0
             DELETE            0            0          0          0
             UPDATE            0            0          0          0
          REKEY(IN)            0            0          0          0
         REKEY(OUT)            0            0          0          0

            Ring Name      Read    Write   ReadERR  WriteERR ItemCount
            DCR Ring          0        0         0         0         0
            DDM Ring          0        0         0         0         0
```

show platform software ipsec vesen-event-log

To display a step-by-step history of how security sessions are created, updated, and deleted, use the **show platform software ipsec vesen-event-log** command in privileged EXEC mode.

show platform software ipsec vesen-event-log

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.14.1a	This command was introduced.

Usage Guidelines

Use these commands only on Cisco IOS XE Catalyst SD-WAN devices.

The following is a sample output that shows the step-by-step history of how security sessions are created, updated, and deleted:

```
Device# show platform software ipsec vesen-event-log
urrIndex=8 log_rotated=FALSE AggCount=8, max_entries=8000
  Idx                      Time           Description
    0   2025/06/03 08:46:12.159  CREATE: bfd_ld=20001, tunnel_id=3104768264,
10.1.15.15/12366->10.1.14.14/12346, local public=10.1.15.15/12366, remote
private=10.1.14.14/12346, local sys_ip/color=172.16.255.15/lte, remote
sys_ip/color=172.16.255.14/lte, in/out spi=0x102(258)/0x105(261), auth_ah=0, auth_ah_no_id=0,
 cause=0x0(), sub_cause=0x0()
    1   2025/06/03 08:46:12.218  CREATE DONE: bfd_ld=20001, tunnel_id=3104768264,
10.1.15.15/12366->10.1.14.14/12346, flow_id=0x24000002, out_spi=0x105(261), cause=0x0,
sub_cause=0x0
    2   2025/06/03 08:46:16.287  CREATE: bfd_ld=20002, tunnel_id=3902372632,
10.1.15.15/12366->10.1.16.16/12346, local public=10.1.15.15/12366, remote
```

```
private=10.1.16.16/12346, local sys_ip/color=172.16.255.15/lte, remote
sys_ip/color=172.16.255.16/lte, in/out spi=0x102(258)/0x102(258), auth_ah=0, auth_ah_no_id=0,
 cause=0x0(), sub_cause=0x0()
    3   2025/06/03 08:46:16.293  CREATE DONE: bfd_ld=20002, tunnel_id=3902372632,
10.1.15.15/12366->10.1.16.16/12346, flow_id=0x24000004, out_spi=0x102(258), cause=0x0,
sub_cause=0x0
    4   2025/06/03 08:46:21.151  CREATE: bfd_ld=20003, tunnel_id=1704557336,
10.1.15.15/12366->10.0.5.11/12347, local public=10.1.15.15/12366, remote
private=10.0.5.11/12347, local sys_ip/color=172.16.255.15/lte, remote
sys_ip/color=172.16.255.11/lte, in/out spi=0x102(258)/0x105(261), auth_ah=0, auth_ah_no_id=0,
 cause=0x0(), sub_cause=0x0()
    5   2025/06/03 08:46:21.164  CREATE DONE: bfd_ld=20003, tunnel_id=1704557336,
10.1.15.15/12366->10.0.5.11/12347, flow_id=0x24000006, out_spi=0x105(261), cause=0x0,
sub_cause=0x0
    6   2025/06/03 08:46:26.151  CREATE: bfd_ld=20004, tunnel_id=3902372632,
10.1.15.15/12366->10.0.5.21/12357, local public=10.1.15.15/12366, remote
private=10.0.5.21/12357, local sys_ip/color=172.16.255.15/lte, remote
sys_ip/color=172.16.255.21/lte, in/out spi=0x102(258)/0x105(261), auth_ah=0, auth_ah_no_id=0,
 cause=0x0(), sub_cause=0x0()
    7   2025/06/03 08:46:26.163  CREATE DONE: bfd_ld=20004, tunnel_id=3902372632,
10.1.15.15/12366->10.0.5.21/12357, flow_id=0x24000008, out_spi=0x105(261), cause=0x0,
sub_cause=0x0
```

show platform software memory

To display memory information for a specified process, use the **show platform software memory** command in privileged EXEC mode or diagnostic mode.

show platform software memory [**database**] *process slot* **alloc** *parameter* [**brief**]

Syntax Description

database	(Optional) Displays database memory information for the specified process.
process	A message process. Valid values: • cfgmgr: Configuration manager process • cxpd: Cloud Express process used for Microsoft Office 365 • dbgd: Speed test process • fpmd: Forwarding Policy manager process • ftm: Forwarding table manager process • ompd: Overlay management protocol daemon process • ttmd: Tunnel manager process • vdaemon: vDeamon process
slot	Hardware slot from which process messages must be logged. Valid values: • rp active: Active RP • r0: Slot 0

statistics	Message statistics. Valid values: • callsite: CallSite display • type component: Component-based memory statistics • type data: Data type based memory statistics • backtrace: Backtrace display
brief	(Optional) Displays abbreviated output.

Command Default

This command has no default behavior.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Support was added for Cisco Catalyst SD-WAN processes.

Usage Guidelines

You can use the **debug platform software memory ftm rp active alloc** command in privileged EXEC mode to start, stop, or clear callsite or backtrace tracking.

Example

The following example shows how to display software platform memory for active RPs at CallSites:

```
Device# show platform software memory ftm rp active alloc callsite
callsite: 1079865346, thread_id: 7921
allocs: 10, frees: 1, alloc_bytes: 1239, free_bytes: 40, call_diff: 9, byte_diff: 1199
callsite: 276369408, thread_id: 7921
allocs: 1, frees: 0, alloc_bytes: 16960, free_bytes: 0, call_diff: 1, byte_diff: 16960
callsite: 279023616, thread_id: 7921
allocs: 1, frees: 0, alloc_bytes: 57360, free_bytes: 0, call_diff: 1, byte_diff: 57360
callsite: 1079865349, thread_id: 7921
allocs: 3, frees: 2, alloc_bytes: 4560, free_bytes: 3040, call_diff: 1, byte_diff: 1520
callsite: 1347823618, thread_id: 7921
allocs: 1, frees: 0, alloc_bytes: 1536, free_bytes: 0, call_diff: 1, byte_diff: 1536
callsite: 1347823619, thread_id: 7921
allocs: 1, frees: 0, alloc_bytes: 40, free_bytes: 0, call_diff: 1, byte_diff: 40
callsite: 1347823620, thread_id: 7921
allocs: 1, frees: 0, alloc_bytes: 8208, free_bytes: 0, call_diff: 1, byte_diff: 8208
callsite: 279746563, thread_id: 7921
allocs: 1, frees: 0, alloc_bytes: 336, free_bytes: 0, call_diff: 1, byte_diff: 336
callsite: 279746564, thread_id: 7921
allocs: 1, frees: 0, alloc_bytes: 57384, free_bytes: 0, call_diff: 1, byte_diff: 57384
callsite: 2156775457, thread_id: 7921
allocs: 1, frees: 0, alloc_bytes: 1688, free_bytes: 0, call_diff: 1, byte_diff: 1688
callsite: 1348148375, thread_id: 7921
allocs: 1, frees: 0, alloc_bytes: 40, free_bytes: 0, call_diff: 1, byte_diff: 40
callsite: 3492619269, thread_id: 7921
allocs: 1, frees: 0, alloc_bytes: 32, free_bytes: 0, call_diff: 1, byte_diff: 32
callsite: 1348148376, thread_id: 7921
allocs: 1, frees: 0, alloc_bytes: 35, free_bytes: 0, call_diff: 1, byte_diff: 35
callsite: 1348148377, thread_id: 7921
allocs: 1, frees: 0, alloc_bytes: 40, free_bytes: 0, call_diff: 1, byte_diff: 40
```

```
callsite: 3492619268, thread_id: 7921
allocs: 1, frees: 0, alloc_bytes: 88, free_bytes: 0, call_diff: 1, byte_diff: 88
```

The following example shows how to display component-based memory statistics for active RPs:

```
Device# show platform software memory ftm rp active alloc type component
Module: vista
   Allocated: 541300, Requested: 540292, Overhead: 1008
   Allocations: 18, Null Allocations: 0, Frees: 0
 Module: bmalloc
   Allocated: 167591, Requested: 160647, Overhead: 6944
   Allocations: 940, Null Allocations: 0, Frees: 816
 Module: systime
   Allocated: 72, Requested: 16, Overhead: 56
   Allocations: 1, Null Allocations: 0, Frees: 0
 Module: tdllib_c
   Allocated: 1584, Requested: 1304, Overhead: 280
   Allocations: 6, Null Allocations: 0, Frees: 1
 Module: chasfs
   Allocated: 13046, Requested: 12542, Overhead: 504
   Allocations: 19, Null Allocations: 0, Frees: 10
 Module: pcohort
   Allocated: 654, Requested: 206, Overhead: 448
   Allocations: 13, Null Allocations: 0, Frees: 5
 Module: vs_lock
   Allocated: 840, Requested: 672, Overhead: 168
   Allocations: 3, Null Allocations: 0, Frees: 0
 Module: flashlib
   Allocated: 7920, Requested: 7864, Overhead: 56
   Allocations: 1, Null Allocations: 0, Frees: 0
 Module: default
   Allocated: 4450977, Requested: 4243329, Overhead: 207648
   Allocations: 32752, Null Allocations: 0, Frees: 29044
 Module: lib
   Allocated: 0, Requested: 0, Overhead: 0
   Allocations: 6, Null Allocations: 0, Frees: 6
```

show platform software nat66 fp active

To verify the NAT66 forwarding processor information, use the **show platform software nat66 fp active prefix-translation** command in privileged EXEC mode.

show platform software nat66 fp active { configuration | interface | prefix-translation | statistics }

Syntax Description

configuration	Displays configuration information for the forwarding processor.
interface	Displays interface information.
prefix-translation	Displays prefix-translation information.
statistics	Displays statistics from the forwarding processor.

Command Default

No NAT66 forwarding processor information is displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Examples

The following is a sample output from the **show platform software nat66 fp active** command:

```
Device# show platform software nat66 fp active interface
NAT66 Interface:
IF Handle 7:
  Enabled TRUE , Inside FALSE
IF Handle 10:
  Enabled TRUE , Inside FALSE
```

show platform software nat66 rp active

To verify the NAT66 route processor (RP) information, use the **show platform software nat66 rp active** command in privileged EXEC mode.

show platform software nat66 rp active { interface | prefix-translation }

Syntax Description

interface	Displays interface information.
prefix-translation	Displays prefix-translation information.

Command Default

No NAT66 route processor information is displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Examples

The following is a sample output from the **show platform software nat66 rp active** command:

```
Device# show platform software nat66 rp active interface


NAT66 Interface:
IF Handle 7:
  Enabled TRUE , Inside FALSE
IF Handle 10:
Enabled TRUE , Inside FALSE
```

show platform software sdwan ftmd bridge-domain

To display the current configuration and status of all bridge domains on the Cisco Catalyst SD-WAN Forwarding and Timing Module Daemon (FTMD), use the **show platform software sdwan ftmd bridge-domain** command in privileged EXEC mode.

show platform software sdwan ftmd bridge-domain [*bridge-domain-id*]

Syntax Description

bridge-domain-id	Lists the bridge-domain information in FTM for a specific bridge domain.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.14.1a	This command was introduced.

Usage Guidelines

Use these commands only on Cisco IOS XE Catalyst SD-WAN devices.

The following is a sample output that shows all bridge domains:

```
Device# show platform software sdwan ftmd bridge-domain
L2vpn Bridge-domain 12 Table:
  sdwan efp dpidx: 4210708(0x404014)
  Label: 1004 lbl-nhop-id: 196611 (binosId=0xf830003f)
  Bum Label: 1005 bum-lbl-nhop-id: 196612 (binosId=0xf830004f)
  Remote Site Table(1 entries in total):
    remote-site-id: 501 sla-nhop-id: 29 (binosId=0xf80001df)
L2vpn Bridge-domain 13 Table:
  sdwan efp dpidx: 4210709(0x404015)
  Label: 1006 lbl-nhop-id: 196613 (binosId=0xf830005f)
  Bum Label: 1007 bum-lbl-nhop-id: 196614 (binosId=0xf830006f)
  Remote Site Table(2 entries in total):
    remote-site-id: 501 sla-nhop-id: 30 (binosId=0xf80001ef)
remote-site-id: 503 sla-nhop-id: 33 (binosId=0xf800021f)
```

The following is a sample output that shows a specific bridge-domain:

```
Device# show platform software sdwan ftmd bridge-domain 13
L2vpn Bridge-domain 13 Table:
  sdwan efp dpidx: 4210709(0x404015)
  Label: 1006 lbl-nhop-id: 196613 (binosId=0xf830005f)
  Bum Label: 1007 bum-lbl-nhop-id: 196614 (binosId=0xf830006f)
  Remote Site Table(2 entries in total):
    remote-site-id: 501 sla-nhop-id: 30 (binosId=0xf80001ef)
    remote-site-id: 503 sla-nhop-id: 33 (binosId=0xf800021f)
```

show platform software sdwan multicast active-sources vrf

To view the entries for a specific Cisco IOS XE SD-WAN multicast active sources on VRF node, use the **show platform software sdwan multicast active-sources vrf** command in privileged EXEC mode.

show platform software sdwan multicast active-sources vrf *vrf-id*

Syntax Description

vrf *vrf-id*	Displays hardware entry information that is based on the specified virtual routing and forwarding (VRF) ID. Valid values are from 1 to 65530.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.15.1a	This command was introduced.

Usage Guidelines

Use this command to view hardware information based on the specified VRF value, and to verify that system IP addresses are configured with spt-only mode.

Examples

The following is sample output from the **show platform software sdwan multicast active-sources vrf** command:

```
Device# show platform software sdwan multicast active-sources vrf 1

Multicast SDWAN Overlay Received Source-Active Routes:
  (10.0.0.0, 255.0.0.0) src-orig: 192.168.0.0, next-hop: 192.168.255.254
      src-orig-count: 1, rp-addr: 10.0.0.1
```

show platform software sdwan multicast remote-nodes vrf

To view the entries for a specific Cisco IOS XE SD-WAN multicast remote node, use the **show platform software sdwan multicast remote-nodes vrf** command in privileged EXEC mode.

show platform software sdwan multicast remote-nodes vrf *vrf-id*

Syntax Description

vrf *vrf-id*	Displays hardware entry information that is based on the specified virtual routing and forwarding (VRF) ID. Valid values are from 1 to 65530.

Command Default

None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines Use this command to view hardware information based on the specified VRF value, and to verify that system IP addresses are configured with spt-only mode.

Examples The following is sample output from the **show platform software sdwan multicast remote-nodes vrf** command:

```
Device# show platform software sdwan multicast remote-nodes vrf 1

Multicast SDWAN Overlay Remote Nodes (* - Replicator):
                                          Received                Sent
                SPT-Only                (X,G)       (S,G)       (X,G)       (S,G)
System IP       Mode         Label   Join/Prune Join/Prune Join/Prune Join/Prune
172.16.255.11   Yes          1003        0/0        0/0        0/0        0/0
172.16.255.14   Yes          1003        0/0        0/0        1/0       10/10
172.16.255.16   Yes          1003        0/0        0/0        0/0        0/0
172.16.255.21   Yes          1003        0/0        0/0        0/0        0/0
```

show platform software sdwan qos

To display Quality of Service (QoS) information, such as QoS configuration, policies, and statistics, use the **show platform software sdwan qos** command in privileged EXEC mode.

show platform software sdwan qos
adapt { **history** { **Dialer** *interface-number* | **GigabitEthernet** *gigabitethernet-interface-number* | **Tunnel** *tunnel-interface-number* | **all** } | **stats** } | **policy** | **target** | **template** | **summary**

Syntax Description

adapt Show adaptive QoS information.

- **history**: Show adaptive QoS history information.
  - **Dialer** *interface-number*: Dialer interface number

    Range: 0 through 255
  - **GigabitEthernet** *gigabitethernet-interface-number*: GigabitEthernet interface number

    Range: 1 through 32
  - **Tunnel** *tunnel-interface-number*: Tunnel interface number

    Range: 1 through 2147483647
  - **all**: All adaptive QoS history information, including dialer, GigabitEthernet, and tunnel information.
- **stats**: Show adaptive QoS statistics information.

policy	Show session QoS policy-map information.
target	Show session QoS target information.
template	Show session QoS template information.
summary	Show a summary of session QoS database information.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.13.1a	Added the **summary** and **sessions** keywords.

Example

Confirm the count of sessions, policies, WAN interfaces, and adaptive QoS sessions.

```
Device# show platform software sdwan qos summary
============ Session QoS Summary Database ============
maximum sdwan qos session support : 2000
number of qos wan interfaces : 2
number of sdwan session qos installed : 2000
number of adaptive qos session installed : 0
number of sdwan policy-map instances : 400
```

Verifies the count of reuse policies. Count of reuse policies refers to the number of policies that are being reused across the network.

```
Device# show platform software sdwan qos policy
============ Session QoS Policy Database ============
policy bandwidth remaining-ratio template sessions
SDWANPolicy4210705 101600000 10 qos_policy_4class 5
SDWANPolicy4210707 101800000 10 qos_policy_4class 5
SDWANPolicy4210709 307802000 30 qos_policy_4class 5
SDWANPolicy4210711 308002000 30 qos_policy_4class 5
SDWANPolicy4210713 308202000 30 qos_policy_4class 5
SDWANPolicy4210715 308402000 30 qos_policy_4class 5
SDWANPolicy4210717 308602000 30 qos_policy_4class 5
SDWANPolicy4210719 308802000 30 qos_policy_4class 5
SDWANPolicy4210721 309802000 30 qos_policy_4class 5
```

Provides the number of sessions allowed per WAN interface.

```
Device# show platform software sdwan qos template
============ Session QoS Template Database ============
interface name interface id QoS template name sessions
GigabitEthernet1 7 qos_policy_4class 1000
GigabitEthernet4 10 qos_policy_4class 1000
```

Provides information about all the session details.

```
Device# show platform software sdwan qos target
============ Session QoS Target Database ============
src-addr               dst-addr            sport   dport   proto remote-tloc    dummy-intf
           tunnel         policy                bandwidth
10.0.0.8              192.0.2.254            12346   12346   IPSEC 10.0.0.6
```

```
SDWANSession4212705   Tunnel1        SDWANPolicy4212007    203401
10.0.0.8               192.0.2.254           12346   12346   IPSEC 10.0.0.6
SDWANSession4212707   Tunnel1        SDWANPolicy4211995    208801
10.0.0.8               192.0.2.254           12346   12346   IPSEC 10.0.0.6
SDWANSession4212709   Tunnel1        SDWANPolicy4211937    206001
10.0.0.8               192.0.2.254           12346   12346   IPSEC 10.0.0.6
SDWANSession4212711   Tunnel1        SDWANPolicy4211939    206201
10.0.0.8               192.0.2.254           12346   12346   IPSEC 10.0.0.6
SDWANSession4212713   Tunnel1        SDWANPolicy4211941    206401
10.0.0.8               192.0.2.254           12346   12346   IPSEC 10.0.0.6
SDWANSession4212715   Tunnel1        SDWANPolicy4211961    204001
10.0.0.8               192.0.2.254           12346   12346   IPSEC 10.0.0.6
SDWANSession4212717   Tunnel1        SDWANPolicy4211973    204201
```

show platform software sdwan tloc-db

To display the database of TLOCs and their associated security information as maintained in the IOS layer, use the **show platform software sdwan tloc-db** command in privileged EXEC mode.

show platform software sdwan tloc-db

Syntax Description

This command has no keywords or arguments.

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 26.1.1	This command was introduced.

Usage Guidelines Use these commands only on Cisco IOS XE Catalyst SD-WAN devices.

The following is a sample output that shows all the database of TLOCs and their associated security information:

```
Device# show platform software sdwan tloc-db
L======TLOC Database=====
SYS-ip              color               encap   Origin TLOC-index  Gen-id
10.0.1.1            gold                IPSEC   REMOTE 32777 2147483648
10.0.1.1            silver              IPSEC   REMOTE 32776 2147483648
10.0.1.2            mpls                IPSEC   LOCAL  32772 2147483697
10.0.1.2            gold                IPSEC   LOCAL  32773 2147483697
10.0.1.2            silver              IPSEC   LOCAL  32771 2147483697
10.0.1.2            bronze              IPSEC   LOCAL  32770 2147483697
```

show platform software sdwan ttmd local-tlocs

To inspect the TLOC Table Manager (TTM) database for local TLOCs, use the **show platform software sdwan ttmd local-tlocs** command in privileged EXEC mode.

show platform software sdwan ttmd local-tlocs

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.14.1a	This command was introduced.

Usage Guidelines

Use these commands only on Cisco IOS XE Catalyst SD-WAN devices.

The following is a sample output that shows the details of the TTM database for local TLOCs:

```
Device# show platform software sdwan ttmd local-tlocs
================================
      TTM Local TLOC Database
  ================================

Local TLOC DB for Tenant ([Default]/0)

TTM-Entry: (0x579feecf1f38), TLOC-IPV4, Tenant: 0, Owner: vdaemon_0, Flags: (0x0)
    TLOC: 10.0.1.2 : gold : ipsec, Origin: LOCAL, Index: 32770, Phy Index: 0, flags: 0x0
    Carrier: 1, LR Enabled: 0, LR hold time: 7000    TLOC Attrs Modified Route:  FALSE,
Security : TRUE         <----- Check which OMP attribute is modified
    Status: Up, Active: No, BFD Handle: 0, BFD Status: UP
    Attributes: Flags: (0x8012e0fe43a6) Flags 2: (0x0) GROUP PREF WEIGHT GEN-ID VERSION
TLOCv4-PUB TLOCv4-PRI TLOCv6-PUB TLOCv6-PRI SITE-ID CARRIER ENCAP SECURITY RESTRICT ON-DEMAND
 BANDWIDTH ADAPT_QOS QOS_GROUP CAP IPV6_STRICT_CONTROL
        Pref: 0, Weight: 1, site-id: 2, region-id: 65534, sec-region-id: 65535,
orig-access-region-id: 65534, Stale: 0
        Ver: 3, Gen-id: 2147483648, Restrict: 0, On-Demand: 0, Border: 0 Mgmt-Region:0
        Group-count 1
        Group-List: 0
        Bandwidth 0
        Bandwidth_dMin 0
        Bandwidth_Down 0
        Bandwidth_dMax 0
        Adapt QoS Period 0
        Adapt QoS Up 0
        Qos_Group default-group
        Capability 0x3f
        TLOCv4-Public: 10.1.1.2:12346
        TLOCv4-Private: 10.1.1.2:12346
        TLOCv6-Public: :::0
        TLOCv6-Private: :::0
```

```
Encap: ipsec-tunnel, Integrity: ip-udp-esp esp(0x98), encrypt: aes256(0xc), spi 260

   ckey: *****2cd1 akey: *****2cd1
```

show platform software sdwan ttmd history tloc

To view more historical details for specific TLOCs, use the **show platform software sdwan ttmd history tloc** command in privileged EXEC mode.

show platform software sdwan ttmd history tloc

Syntax Description

This command has no keywords or arguments.

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.15.1a	This command was introduced.

Usage Guidelines Use these commands only on Cisco IOS XE Catalyst SD-WAN devices.

The following is a sample output that shows the historical details for specific TLOCs:

```
Device# show platform software sdwan ttmd history tloc 0 12.16.255.12 mpls ipsec

8      Wed Mar 18 20:52:08 2026:50   [0] : AF: 00 IP: 12.16.255.12 Color: mpls Encap: ipsec
 : Origin: Remote Client: OMPD Event: CREATE Flags: 0 Attr: 8012e0fe43a6
7      Wed Mar 18 20:52:08 2026:50   [0] : AF: 00 IP: 12.16.255.12 Color: mpls Encap: ipsec
 : Origin: Remote Client: OMPD Event:    ADD Flags: 0 Attr: 8012e0fe43a6
6      Wed Mar 18 20:52:08 2026:51   [0] : AF: 00 IP: 12.16.255.12 Color: mpls Encap: ipsec
 : Origin: Remote Client: ftmd Event:    ADD Flags: 0 Attr: 8012e0fe43a6
5      Wed Mar 18 20:52:08 2026:51   [0] : AF: 00 IP: 12.16.255.12 Color: mpls Encap: ipsec
 : Origin: Remote Client: fpmd Event:    ADD Flags: 0 Attr: 8012e0fe43a6
4      Wed Mar 18 20:52:08 2026:159  [0] : AF: 00 IP: 12.16.255.12 Color: mpls Encap: ipsec
 : Origin: Remote Client: OMPD Event: UPDATE Flags: 0 Attr: 8012e0fe43a6
3      Wed Mar 18 20:52:08 2026:159  [0] : AF: 00 IP: 12.16.255.12 Color: mpls Encap: ipsec
 : Origin: Remote Client: OMPD Event: UPD_IG Flags: 0 Attr: 8012e0fe43a6
2      Wed Mar 18 20:52:09 2026:824  [0] : AF: 00 IP: 12.16.255.12 Color: mpls Encap: ipsec
 : Origin: Remote Client: ftmd Event: BFD_ST Flags: 0 Attr: 8012e0fe43a6
1      Wed Mar 18 20:52:09 2026:826  [0] : AF: 00 IP: 12.16.255.12 Color: mpls Encap: ipsec
 : Origin: Remote Client: OMPD Event:    ADD Flags: 0 Attr: 8012e0fe43a6
0      Wed Mar 18 20:52:09 2026:826  [0] : AF: 00 IP: 12.16.255.12 Color: mpls Encap: ipsec
 : Origin: Remote Client: fpmd Event:    ADD Flags: 0 Attr: 8012e0fe43a6

Displyed aggregated log cnt 9 from log-types

[00:172.16.255.12:mpls:ipsec] Max cnt: 40    Data len: 32    Agg cnt: 9     Rotated: NO
Current index: 9
```

show platform software sdwan ttmd tlocs stats

To display the statistics on TLOC creation, updates, and attribute modifications, use the **show platform software sdwan ttmd tlocs stats** command in privileged EXEC mode.

show platform software sdwan ttmd tlocs stats

Syntax Description

This command has no keywords or arguments.

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 26.1.1	This command was introduced.

Usage Guidelines Use these commands only on Cisco IOS XE Catalyst SD-WAN devices.

The following is a sample output that shows the statistics on TLOC creation, updates, and attribute modifications:

```
Device# show platform software sdwan ttmd tlocs stats
Local TLOC :

  Create         :: 1
  Update         :: 0
  delete         :: 0
  Route Attr Mod :: 1
  Sec Attr Mod   :: 1
-------------------------
   Remote  TLOC:

  Create         :: 1
  Update         :: 1
  delete         :: 0
  Route Attr Mod :: 2
  Sec Attr Mod   :: 3
```

show policy-firewall config

To validate the configured zone based firewall, use the **show policy-firewall config** command in user EXEC or privileged EXEC mode command in user EXEC or privileged EXEC mode.

show policy-firewall config

Command Default None

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

The following sample outputs displays the configured firewall policy.

```
Device# show policy-firewall config
Zone-pair              : ZP_SRC_INTF1_DIA_INTF_TEST
Source Zone            : SRC_INTF1
  Member Interfaces:
    GigabitEthernet3.101
Destination Zone       : DIA_INTF
  Member Interfaces:
    GigabitEthernet1
    GigabitEthernet2
    GigabitEthernet4
Service-policy inspect : TEST-opt
  Class-map : TEST-seq-1-cm_ (match-all)
   Match access-group name TEST-seq-Rule_1-acl_
  Action : inspect
   Parameter-map : Default
  Class-map : TEST-seq-11-cm_ (match-all)
   Match access-group name TEST-seq-Rule_2-acl_
  Action : inspect
   Parameter-map : Default
  Class-map : class-default (match-any)
   Match any
  Action : drop log
   Parameter-map : Default
```

show policy-map interface Port-channel

To monitor and troubleshoot Quality of Service (QoS) issues on a port-channel interface, use the **show policy-map interface Port-channel** command in privileged EXEC mode.

show policy-map interface Port-channel

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.13.1a	This command is supported for Cisco Catalyst SD-WAN.

Examples

The following is a sample output from the **show policy-map interface Port-channel** command that is used to monitor and troubleshoot Quality of Service (QoS) issues on a port channel interface:

```
Device# show policy-map interface Port-channel 1
Port-channel1
```

```
Service-policy output: shape_Port-channel1

  Class-map: class-default (match-any)
    121 packets, 20797 bytes
    5 minute offered rate 2000 bps, drop rate 0000 bps
    Match: any
    Queueing
    queue limit 416 packets
    (queue depth/total drops/no-buffer drops) 0/0/0
    (pkts output/bytes output) 121/20797
    shape (average) cir 100000000, bc 400000, be 400000
    target shape rate 100000000

    Service-policy : qos_template

      queue stats for all priority classes:
        Queueing
        priority level 1
        queue limit 512 packets
        (queue depth/total drops/no-buffer drops) 0/0/0
        (pkts output/bytes output) 121/20797

      Class-map: Critical (match-any)
        121 packets, 20797 bytes
        5 minute offered rate 2000 bps, drop rate 0000 bps
        Match: qos-group 0
        police:
            rate 15 %
            rate 15000000 bps, burst 468750 bytes
          conformed 121 packets, 20797 bytes; actions:
            transmit
          exceeded 0 packets, 0 bytes; actions:
            drop
          conformed 2000 bps, exceeded 0000 bps
        Priority: Strict, b/w exceed drops: 0

        Priority Level: 1

      Class-map: Business (match-any)
        0 packets, 0 bytes
        5 minute offered rate 0000 bps, drop rate 0000 bps
        Match: qos-group 1
        Queueing
        queue limit 416 packets
        (queue depth/total drops/no-buffer drops) 0/0/0
        (pkts output/bytes output) 0/0
        bandwidth remaining 55%

      Class-map: Best-Effort (match-any)
        0 packets, 0 bytes
        5 minute offered rate 0000 bps, drop rate 0000 bps
        Match: qos-group 2
        Queueing
        queue limit 416 packets
        (queue depth/total drops/no-buffer drops) 0/0/0
        (pkts output/bytes output) 0/0
        bandwidth remaining 10%

      Class-map: Bulk (match-any)
        0 packets, 0 bytes
        5 minute offered rate 0000 bps, drop rate 0000 bps
        Match: qos-group 3
        Queueing
```

```
  queue limit 416 packets
  (queue depth/total drops/no-buffer drops) 0/0/0
  (pkts output/bytes output) 0/0
  bandwidth remaining 20%

Class-map: class-default (match-any)
  0 packets, 0 bytes
  5 minute offered rate 0000 bps, drop rate 0000 bps
  Match: any

  queue limit 416 packets
  (queue depth/total drops/no-buffer drops) 0/0/0
  (pkts output/bytes output) 0/0
```

show processes cpu platform

To view utilization of the individual control, data, and service planes, use the **show processes cpu platform** command in privileged EXEC mode.

show processes cpu platform [history | location | monitor | profile { CP | DP | SP } | sorted [5sec | 1min | 5min]]

Syntax Description

history	Show CPU usage history of the system.
location	Field-replacable unit (FRU) location. An is a component or module within a network device, such as a router or switch, that can be replaced without needing to send the entire device back to the manufacturer. The FRU location refers to where these units are located within the device.
monitor	Monitor running Cisco IOS XE processes.
profile {**CP** | **DP** | **SP**}	Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Show CPU ulitization per profile. • **CP**: Show CPU usage of control plane. • **DP**: Show CPU usage of data plane. • **SP**: Show CPU usage of service plane.
sorted [**5sec** | **1min** | **5min**]	Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Show sorted output based on percentage of usage for Cisco IOS XE processes. Optionally, you can specify the interval: • **5sec**: (Default) Sort based on a 5-second interval. • **1min**: Sort based on a 1-minute interval. • **5min**: Sort based on a 5-minute interval.

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.13.1a	Added the **profile** and **sorted** options.

Usage Guidelines Some Cisco IOS XE Catalyst SD-WAN devices generate CPU utilization alarms indicating high usage, despite the system functioning in a healthy state. This show command separates the CPU usage and provides a more accurate report of the actual CPU usage on all three planes, the control plane, the data plane, and the service plane.

Note The output of this command reflects the kernel-level CPU utilization for the cores used by the data path. However, this output is not for health monitoring of the data path, or for estimating the current capacity levels for data plane processing. This is due to the nature of processing where the data plane relies on poll-based I/O, and some threads spend CPU resources for receive or transmit of packets. Hence the indicated load does not directly reflect the processing capacity. For example, where a thread may be near 100% CPU utilization, but is processing relatively low traffic rates and have capacity to process much higher rates. To get an accurate view of data plane processing capacity and for data plane health monitoring, use the QFP show command, **show platform hardware qfp active datapath utilization**. Use the **show process cpu platform profile CP** command output to monitor health of the control plane, and the QFP commands to monitor the data plane.

Note The edge devices with greater than 8 GB of memory on Cisco IOS XE Catalyst SD-WAN Release 17.8.1a and later releases provides additional DRAM resources of 512 MB for the QFP in the system.

Example

The following sample outputs of the **show processes cpu platform** command display the CPU utilizations for the control plane, the data plane, and the service plane.

```
Device# show processes cpu platform profile CP
CPU utilization for five seconds: 1%, one minute: 1%, five minutes: 1%
Core 0: CPU utilization for five seconds: 2%, one minute: 1%, five minutes: 1%
Core 1: CPU utilization for five seconds: 2%, one minute: 1%, five minutes: 1%
Core 12: CPU utilization for five seconds: 1%, one minute: 1%, five minutes: 1%
Core 13: CPU utilization for five seconds: 2%, one minute: 1%, five minutes: 1%
Control plane process utilization for five seconds: 5%, one minute: 7%, five minutes: 7%
Pid PPid 5Sec 1Min 5Min Status Size Name
------------------------------------------------------------------------------
9089 8683 0% 0% 0% S 2764 pman
9096 9089 0% 0% 0% S 26332 psd
9367 8683 0% 0% 0% S 2776 pman
9376 9367 1% 1% 1% S 857688 linux_iosd-imag
9595 8683 0% 0% 0% S 2760 pman
...

Device# show processes cpu platform profile DP
CPU utilization for five seconds: 7%, one minute: 9%, five minutes: 9%
Core 2: CPU utilization for five seconds: 3%, one minute: 2%, five minutes: 3%
Core 3: CPU utilization for five seconds: 1%, one minute: 1%, five minutes: 1%
Core 4: CPU utilization for five seconds: 1%, one minute: 1%, five minutes: 1%
```

```
Core 5: CPU utilization for five seconds: 3%, one minute: 5%, five minutes: 5%
Core 6: CPU utilization for five seconds: 2%, one minute: 2%, five minutes: 2%
Core 7: CPU utilization for five seconds: 1%, one minute: 1%, five minutes: 1%
Core 8: CPU utilization for five seconds: 27%, one minute: 35%, five minutes: 36%
Core 9: CPU utilization for five seconds: 31%, one minute: 48%, five minutes: 50%
Core 10: CPU utilization for five seconds: 21%, one minute: 21%, five minutes: 21%
Core 11: CPU utilization for five seconds: 21%, one minute: 22%, five minutes: 22%
Core 14: CPU utilization for five seconds: 1%, one minute: 1%, five minutes: 1%
Core 15: CPU utilization for five seconds: 1%, one minute: 1%, five minutes: 1%
Core 16: CPU utilization for five seconds: 1%, one minute: 1%, five minutes: 1%
Core 17: CPU utilization for five seconds: 1%, one minute: 1%, five minutes: 1%
Core 18: CPU utilization for five seconds: 1%, one minute: 1%, five minutes: 1%
Core 19: CPU utilization for five seconds: 1%, one minute: 1%, five minutes: 1%
Data plane process utilization for five seconds: 171%, one minute: 171%, five minutes: 171%
Pid PPid 5Sec 1Min 5Min Status Size Name
------------------------------------------------------------------------------
15833 15219 0% 0% 0% S 2764 pman
15840 15833 172% 171% 171% S 900668 ucode_pkt_PPE0

Device# show processes cpu platform profile SP
CPU utilization for five seconds: 1%, one minute: 1%, five minutes: 1%
Core 0: CPU utilization for five seconds: 1%, one minute: 1%, five minutes: 1%
```

show policy-map type inspect

To view active firewall sessions, use the **show policy-map type inspect** command in privileged EXEC mode.

show policy-map type inspect

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

The following sample outputs displays the view active firewall sessions.

```
Device# show policy-map type inspect
  Policy Map type inspect optimized FW_POLICY1-opt
    Class FW_POLICY1-seq-1-cm_
      Inspect
    Class class-default

  Policy Map type inspect pm1
    Class cm1
      Inspect
    Class class-default
```

show power

To view historic power usage data, use the **show power** command in privileged EXEC mode..

Supported Parameters

detail	Displays detailed power information.
history	Displays power history information.
inline	Displays inline power status.
usage	Displays power usage information.

Example 1:

The following sample output from the command shows the detailed power information.

The following is a sample output from the **show power detail** command.

```
Router# show power detail
Component Power:
 Slot        Type                Instant   Peak      Budget    Unit      Direction
 --------    ------------------  --------  --------  --------  --------  --------
 P0          PWR-CC1-650WAC       143       152       142       Watts     Input
 P0          PWR-CC1-650WAC       129       136       126       Watts     Output
 P1          PWR-CC1-1000WAC      22        26        19        Watts     Input
 P1          PWR-CC1-1000WAC      3         4         3         Watts     Output
 P2          C8300-FAN-2R         7         12        7         Watts
 POE0        PWR-CC1-MOD-POE      75        80        75        Watts     Input
 POE1        PWR-POE-4450         96        96        96        Watts     Input
 0/1         NIM-ES2-8-P          4         4         4         Watts
 0/2         NIMX-M-1TE-SFP       5         5         5         Watts
 R0          C8300-2N2S-4T2X      43        49        39        Watts

System Power:
 Instant   Peak      Budget    Unit
 --------  --------  --------  --------
 165       176       162       Watts

System Energy:
 Meter Reset Time          Meter Update Time         System Energy in WattSec
 ----------------------    ----------------------    ----------------------------
 2024-08-22 23:13:12 UTC   2024-08-23 21:58:12 UTC   13665000

Metered System Energy:
 Meter Update              Hourly Metered    Metered Energy in WattSec (5min Buckets)

 Time                      Value (WattSec)
 ----------------------    ----------------
------------------------------------------------------------------------------
 2024-08-23 21:58:12 UTC   602100
49800-50100-50100-50100-50100-50400-50400-50700-50100-50100-50100-50100
```

Example 2:

The following sample output from the **show power usage** command shows the power usage information.

```
Router# show power usage
 Slot        Type                Allocation                State
 --------    ------------------  --------------------      ------------
 P0          PWR-CC1-650WAC      144  Watts (Input)        Normal
 P0          PWR-CC1-650WAC      128  Watts (Output)       Normal
 P1          PWR-CC1-1000WAC     23   Watts (Input)        Normal
 P1          PWR-CC1-1000WAC     3    Watts (Output)       Normal
 P2          C8300-FAN-2R        7    Watts                Normal
 POE0        PWR-CC1-MOD-POE     75   Watts (Input)        Normal
```

```
 POE1         PWR-POE-4450          96   Watts (Input)       Normal
 0/1          NIM-ES2-8-P           4    Watts               Normal
 0/2          NIMX-M-1TE-SFP        5    Watts               Normal
 R0           C8300-2N2S-4T2X       45   Watts               Normal

Total inline power: 21 Watts
Total input power: 167 Watts
Total output power: 131 Watts
```

show raw-socket

To display raw socket information use the **show raw-socket** command in privileged EXEC mode.

show raw-socket { **tcp** | **udp** } { **sessions** | **statistic** } [**local**]

Syntax Description

raw-socket	Shows information for raw sockets.
tcp	Shows TCP protocol information.
udp	Shows UDP protocol information.
sessions	Displays session details for the raw socket protocol.
statistic	Provides statistics for the raw socket protocol.
local	Displays the raw socket's locally configured client state information.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.18.1a	This command was introduced.

Example

The following is a sample output of the **show raw-socket udp sessions** command:

```
device# show raw-socket udp sessions
 UDP Sessions
Interface   tty/(Idx)  vrf_name  socket   mode     local_ip_addr  local_port    dest_ip_addr
  dest_port   up_time     idle_time/timeout
   0/3/0    74            0      client  15.1.1.1      15001        15.1.1.2       15002
               00:00:14       00:00:14/300sec
```

The following is a sample output of the **show raw-socket tcp sessions** command:

```
device# show raw-socket tcp sessions
TCP Sessions
Interface   tty/(Idx) vrf_name   socket    mode       local_ip_addr  local_port
dest_ip_addr  dest_port    up_time     idle_time/timeout
 As0/3/0   74           0         server   15.1.1.1    15001          listening
```

```
 0/3/0      74          1          server   15.1.1.1    15001           15.1.1.2    15002
                    00:00:41    00:00:41/300sec
```

The following is a sample output of the **show raw-socket udp sessions local** command:

```
device# show raw-socket udp sessions local
Locally configured UDP client State
Interface  tty  dest_ip    dest_port  local_ip    local_port  state
0/3/0      74   15.1.1.2    15002     15.1.1.1      15001      UP
```

The following is a sample output of the **show raw-socket tcp sessions local** command:

```
device1# show raw-socket tcp sessions local
Locally configured TCP client State
Interface  tty  dest_ip    dest_port  local_ip   local_port  state
0/2/0      26   15.1.1.1    15001     15.1.1.2     15002      UP
```

Note The **show raw-socket tcp session local** command is supported exclusively on the client device.

The following is a sample output of the **show raw-socket udp statistics** command:

```
device# show raw-socket udp statistics
UDP-Serial Statistics
Interface  idx     vrf_name             sessions      udp_in_bytes         udp_out_bytes
 udp_to_tty_frames    tty_to_udp_frame
As0/3/0    74        1                   0                   0                   0
             0
```

The following is a sample output of the **show raw-socket tcp statistics** command:

```
device# show raw-socket tcp statistics
TCP-Serial Statistics
Interface  idx    vrf_name  sessions tcp_in_bytes   tcp_out_bytes   tcp_to_tty_frames
tty_to_tcp_frames
  As0/3/0   74    1             0                   0                   0
    0
```

show redundancy application control-interface group

To display detailed information about the control interfaces used for application redundancy groups on a Cisco IOS XE Catalyst SD-WAN device, use the **show redundancy application control-interface group** command in privileged EXEC mode.

show redundancy application control-interface group [**group-id**]

Syntax Description

group-id	Displays the redundancy group information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.15.1a	This command is supported for Cisco Catalyst SD-WAN.

Usage Guidelines

Use **show redundancy application control-interface group** to display detailed information about the control interface for application redundancy groups on a Cisco IOS XE Catalyst SD-WAN device. The control interface is the network interface used to manage and monitor redundancy operations. This command provides insights into the control interfaces used for redundancy, including their status, configuration details, and any relevant statistics.

Examples

The following is sample output from the **show redundancy application control-interface group** command.

```
Device# show redundancy application control-interface group 1

The control interface for rg[1] is Port-channel1
Interface is Control interface associated with the following protocols: 1
BFD Enabled
Interface Neighbors:
Peer: 10.1.55.14 Active RGs: 2 Standby RGs: 1 BFD handle: 0

The control interface for rg[2] is Port-channel1
Interface is Control interface associated with the following protocols: 1
BFD Enabled
Interface Neighbors:
Peer: 10.1.55.14 Active RGs: 2 Standby RGs: 1 BFD handle: 0
```

show redundancy application data-interface group

To display detailed information about the data interfaces for a specific application redundancy group on a Cisco IOS XE Catalyst SD-WAN device, use the **show redundancy application data-interface group** command in privileged EXEC mode.

show redundancy application data-interface group

Syntax Description

group-id	Displays the redundancy group information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.15.1a	This command is supported for Cisco Catalyst SD-WAN.

Examples

The following is sample output from the **show redundancy application data-interface group** command.

```
Device# show redundancy application data-interface group

The data interface for rg[1] is Port-channel1
The data interface for rg[2] is Port-channel1
```

show redundancy application group

To display information about the redundancy groups configured on a Cisco IOS XE Catalyst SD-WAN device, use the **show redundancy application group** command in privileged EXEC mode.

show redundancy application group

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.15.1a	This command is supported for Cisco Catalyst SD-WAN.

Usage Guidelines

Use the **show redundancy application group** command to view detailed information about the redundancy groups configured on a Cisco IOS XE Catalyst SD-WAN device, showing their RG IDs, RG names, and current states (active or standby). This information helps to monitor and manage high availability and failover configurations effectively.

Examples

The following is sample output from the **show redundancy application group** command. The fields in the display are self-explanatory.

```
Device# show redundancy application group

Group ID    Group Name                     State
--------    ----------                     -----
1           Redundancy-1                  ACTIVE
2           Redundancy-2                  STANDBY
```

The following is a sample output from the **show redundancy application group** command with group id. This command provides information about the specified redundancy application group on a Cisco IOS XE Catalyst SD-WAN device. It includes the administrative and operational states, roles of the current and peer devices, communication status, path optimization, and redundancy framework states.

```
Device# show redundancy application group 1

Group ID:1
Group Name:

Administrative State: No Shutdown
Aggregate operational state : Up
My Role: ACTIVE
Peer Role: STANDBY
Peer Presence: Yes
Peer Comm: Yes
Peer Progression Started: Yes
Path Optimization: Enabled
TLOC Pref Change: 0

RF Domain: btob-one
         RF state: ACTIVE
         Peer RF state: STANDBY HOT
```

The following is a sample output from the **show redundancy application group all** command. This command provides displays the status and details of all application redundancy groups configured

on a Cisco IOS XE Catalyst SD-WAN device. This command provides information about the redundancy groups, including their current state (active or standby), the roles of the devices within each group, and other relevant details necessary for managing and troubleshooting high availability setups.

```
Device# show redundancy application group all

Faults states Group 1 info:
        Runtime priority: [100]
                RG Faults RG State: Up.
                        Total # of switchovers due to faults:           0
                        Total # of down/up state changes due to faults: 2

RG Protocol RG 1
------------------
        Role: Active
        Init Role: Active
        Negotiation Flags 0x1
        Tunnel: UP, DIA: DOWN
        Negotiation: Enabled
        Priority: 100
        Protocol state: Active
        Ctrl Intf(s) state: Up
        Active Peer: Local
        Standby Peer: address 10.1.55.14, priority 100, intf Po1
        Log counters:
                role change to active: 11
                role change to standby: 7
                disable events: rg down state 3, rg shut 0
                ctrl intf events: up 5, down 2, admin_down 1
                reload events: local request 1, peer request 0

RG Media Context for RG 1
--------------------------
        Ctx State: Active
        Protocol ID: 1
        Media type: Default
        Control Interface: Port-channel1
        Current Hello timer: 3000
        Configured Hello timer: 3000, Hold timer: 10000
        Peer Hello timer: 3000, Peer Hold timer: 10000
        Stats:
                Pkts 9982, Bytes 618884, HA Seq 0, Seq Number 9982, Pkt Loss 0
                Authentication not configured
                Authentication Failure: 0
                Reload Peer: TX 0, RX 0
                Resign: TX 3, RX 4
        Standby Peer: Present. Hold Timer: 10000
                Pkts 7365, Bytes 250410, HA Seq 0, Seq Number 9984, Pkt Loss 0


Group ID:1
Group Name:

Administrative State: No Shutdown
Aggregate operational state : Up
My Role: ACTIVE
Peer Role: STANDBY
Peer Presence: Yes
Peer Comm: Yes
Peer Progression Started: Yes
Path Optimization: Enabled
TLOC Pref Change: 0
```

```
RF Domain: btob-one
         RF state: ACTIVE
         Peer RF state: STANDBY HOT

Faults states Group 2 info:
        Runtime priority: [100]
                RG Faults RG State: Up.
                        Total # of switchovers due to faults:           0
                        Total # of down/up state changes due to faults: 0

RG Protocol RG 2
------------------
        Role: Standby
        Init Role: Standby
        Negotiation Flags 0x1
        Tunnel: UP, DIA: DOWN
        Negotiation: Enabled
        Priority: 100
        Protocol state: Standby-hot
        Ctrl Intf(s) state: Up
        Active Peer: address 10.1.55.14, priority 100, intf Po1
        Standby Peer: Local
        Log counters:
                role change to active: 3
                role change to standby: 3
                disable events: rg down state 0, rg shut 0
                ctrl intf events: up 1, down 0, admin_down 0
                reload events: local request 0, peer request 0

RG Media Context for RG 2
--------------------------
        Ctx State: Standby
        Protocol ID: 1
        Media type: Default
        Control Interface: Port-channel1
        Current Hello timer: 3000
        Configured Hello timer: 3000, Hold timer: 10000
        Peer Hello timer: 3000, Peer Hold timer: 10000
        Stats:
                Pkts 7377, Bytes 457374, HA Seq 0, Seq Number 7377, Pkt Loss 0
                Authentication not configured
                Authentication Failure: 0
                Reload Peer: TX 0, RX 0
                Resign: TX 3, RX 2
        Active Peer: Present. Hold Timer: 10000
                Pkts 7157, Bytes 243338, HA Seq 0, Seq Number 7374, Pkt Loss 0


Group ID:2
Group Name:

Administrative State: No Shutdown
Aggregate operational state : Up
My Role: STANDBY
Peer Role: ACTIVE
Peer Presence: Yes
Peer Comm: Yes
Peer Progression Started: Yes
Path Optimization: Enabled
TLOC Pref Change: 0

RF Domain: btob-two
         RF state: STANDBY HOT
         Peer RF state: ACTIVE
```

show redundancy application group protocol

To display information about the redundancy protocol for application redundancy groups configured on a Cisco IOS XE Catalyst SD-WAN device, use the **show redundancy application group protocol** command in privileged EXEC mode.

show redundancy application group protocol

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.15.1a	This command is supported for Cisco Catalyst SD-WAN.

Usage Guidelines

Use the **show redundancy application group protocol** to display detailed information about the redundancy protocol for application redundancy groups configured on a Cisco IOS XE Catalyst SD-WAN device. This command provides insights into the protocol-specific settings and status, which can include the current state of the redundancy protocol, the synchronization status, and other protocol-related details necessary for managing and troubleshooting high availability configurations.

Examples

The following is sample output from the **show redundancy application group protocol** command.

```
Device# show redundancy application group protocol

RG Protocol RG 1
------------------
        Role: Active
        Init Role: Active
        Negotiation Flags 0x1
        Tunnel: UP, DIA: DOWN
        Negotiation: Enabled
        Priority: 100
        Protocol state: Active
        Ctrl Intf(s) state: Up
        Active Peer: Local
        Standby Peer: address 10.1.55.14, priority 100, intf Po1
        Log counters:
                role change to active: 11
                role change to standby: 7
                disable events: rg down state 3, rg shut 0
                ctrl intf events: up 5, down 2, admin_down 1
                reload events: local request 1, peer request 0

RG Media Context for RG 1
--------------------------
        Ctx State: Active
        Protocol ID: 1
        Media type: Default
        Control Interface: Port-channel1
        Current Hello timer: 3000
        Configured Hello timer: 3000, Hold timer: 10000
        Peer Hello timer: 3000, Peer Hold timer: 10000
        Stats:
                Pkts 10001, Bytes 620062, HA Seq 0, Seq Number 10001, Pkt Loss 0
                Authentication not configured
                Authentication Failure: 0
```

```
                Reload Peer: TX 0, RX 0
                Resign: TX 3, RX 4
        Standby Peer: Present. Hold Timer: 10000
                Pkts 7385, Bytes 251090, HA Seq 0, Seq Number 10004, Pkt Loss 0


RG Protocol RG 2
------------------
        Role: Standby
        Init Role: Standby
        Negotiation Flags 0x1
        Tunnel: UP, DIA: DOWN
        Negotiation: Enabled
        Priority: 100
        Protocol state: Standby-hot
        Ctrl Intf(s) state: Up
        Active Peer: address 10.1.55.14, priority 100, intf Po1
        Standby Peer: Local
        Log counters:
                role change to active: 3
                role change to standby: 3
                disable events: rg down state 0, rg shut 0
                ctrl intf events: up 1, down 0, admin_down 0
                reload events: local request 0, peer request 0

RG Media Context for RG 2
--------------------------
        Ctx State: Standby
        Protocol ID: 1
        Media type: Default
        Control Interface: Port-channel1
        Current Hello timer: 3000
        Configured Hello timer: 3000, Hold timer: 10000
        Peer Hello timer: 3000, Peer Hold timer: 10000
        Stats:
                Pkts 7396, Bytes 458552, HA Seq 0, Seq Number 7396, Pkt Loss 0
                Authentication not configured
                Authentication Failure: 0
                Reload Peer: TX 0, RX 0
                Resign: TX 3, RX 2
        Active Peer: Present. Hold Timer: 10000
                Pkts 7177, Bytes 244018, HA Seq 0, Seq Number 7394, Pkt Loss 0
```

show redundancy rii

To display detailed information about the Redundancy Interface Identifiers (RII) on a Cisco IOS XE Catalyst SD-WAN device, use the **show redundancy rii** command in privileged EXEC mode.

show redundancy rii

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.15.1a	This command is supported for Cisco Catalyst SD-WAN.

Usage Guidelines

Use the **show redundancy rii** to display specific RII values assigned to interfaces, indicating how these interfaces are mapped and associated with RIIs.

Examples

The following is sample output from the **show redundancy rii** command.

```
Device# show redundancy rii
No. of RIIs in database: 10
 Interface                        RII Id     decrement
  GigabitEthernet3.104          :   2049          0
  GigabitEthernet3.103          :   2050          0
  GigabitEthernet3.102          :   2051          0
  GigabitEthernet7              :   2053          0
  GigabitEthernet3.105          :   2054          0
  Tunnel2                       :   513           0
  Tunnel1                       :   514           0
  GigabitEthernet3.101          :   2052          0
  GigabitEthernet2              :   1             0
  GigabitEthernet1              :   2             0
```

show sd-routing certificate staged

To display the certificate currently in the staging process on a device in the SD-Routing device solution, use the **show sd-routing certificate staged** command in EXEC mode.

show sd-routing certificate staged

Command Default

This command has no default behavior.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.18.1a	This command was introduced.

Usage Guidelines

For information about staging certificates, see How Cisco SD-WAN Manager installs a new certificate on an edge device in the *Cisco Catalyst SD-WAN Getting Started Guide*.

This command applies to WAN edge devices in the SD-Routing device solution. For devices in the SD-WAN device solution, see show sdwan certificate staged, on page 1328.

While a device has a certificate in staging, which can take a minute or more, this command displays the certificate details. After the device completes the staging and testing of the certificate, the certificate is cleared and the command output does not show a certificate.

Example

This example shows the output of the command when a certificate is in staging. The output is abbreviated.

```
Device#show sd-routing certificate staged
Staged certificate
------------------------------
```

```
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number:
            04:4d:…
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, ST = CA, L = San Jose, OU = Acme, O = Cisco Systems Inc, CN = ca
        Validity
            Not Before: Sep 20 16:52:32 2024 GMT
            Not After : Sep 18 16:52:32 2034 GMT
        Subject: C = US, ST = CA, L = San Jose, OU = Acme, O = Cisco Systems Inc, CN = ce5
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:aa:11:bb:22:cc:33:dd:44:ee:55:ff:66:77:88:
                    …
```

Related Commands

Command	Description
show sdwan certificate staged	Display the certificate currently in the staging process on a device in the SD-WAN device solution.

show sdwan alarms detail

To view detailed information about each alarm separated by a new line, use the **show sdwan alarms detail** command in privileged EXEC mode. This command provides better readability into the alarms.

show sdwan alarms detail

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.12.x	This command was introduced.

Examples

The following is a sample output of the **show sdwan alarms detail** command:

```
vm5#show sdwan alarms detail

alarms 2023-06-01:00:38:46.868569
 event-name     geo-fence-alert-status
 severity-level minor
 host-name      Router
 kv-pair        [ system-ip=:: alert-type=device-tracking-stop alert-msg=Device Tracking
stopped in Geofencing Mode latitude=N/A longitude=N/A geo-color=None ]
------------------------------------------------------

alarms 2023-06-01:00:38:47.730907
 event-name     system-reboot-complete
 severity-level major
```

```
 host-name      Router
 kv-pair        [ ]
-----------------------------------------------------

alarms 2023-06-01:00:39:00.633682
 event-name     pki-certificate-event
 severity-level critical
 host-name      Router
 kv-pair        [ trust-point=Trustpool event-type=pki-certificate-install
valid-from=2008-11-18T21:50:24+00:00 expires-at=2033-11-18T21:59:46+00:00 is-ca-cert=true
subject-name=cn=Cisco Root CA M1,o=Cisco issuer-name=cn=Cisco Root CA M1,o=Cisco
serial-number=2ED20E7347D333834B4FDD0DD7B6967E ]
-----------------------------------------------------
```

show sdwan alarms summary

To view alarm details such as the timestamp, event name, and severity in a tabular format, use the **show sdwan alarms summary** command in privileged EXEC mode. This command provides better readability into the alarms.

show sdwan alarms summary

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.12.x	This command was introduced.

Examples

The following is a sample output of the **show sdwan alarms summary** command:

```
vm5#show sdwan alarms summary

time-stamp                    event-name                                    severity-l

-------------------------------------------------------------------------------------
2023-06-01:00:38:46.868569      geo-fence-alert-status                        minor

2023-06-01:00:38:47.730907      system-reboot-complete                        major

2023-06-01:00:39:00.633682      pki-certificate-event                       critical

2023-06-01:00:39:00.644209      pki-certificate-event                       critical

2023-06-01:00:39:00.649363      pki-certificate-event                       critical

2023-06-01:00:39:00.652777      pki-certificate-event                       critical

2023-06-01:00:39:00.658387      pki-certificate-event                       critical

2023-06-01:00:39:00.661119      pki-certificate-event                       critical

2023-06-01:00:39:00.665882      pki-certificate-event                       critical
```

```
2023-06-01:00:39:00.669655      pki-certificate-event                    critical
2023-06-01:00:39:00.674912      pki-certificate-event                    critical
2023-06-01:00:39:00.683510      pki-certificate-event                    critical
2023-06-01:00:39:00.689850      pki-certificate-event                    critical
2023-06-01:00:39:00.692883      pki-certificate-event                    critical
2023-06-01:00:39:00.699143      pki-certificate-event                    critical
2023-06-01:00:39:00.702386      pki-certificate-event                    critical
2023-06-01:00:39:00.703653      pki-certificate-event                    critical
2023-06-01:00:39:00.704488      pki-certificate-event                    critical
2023-06-01:00:39:01.949479      pki-certificate-event                    critical
2023-06-01:00:40:38.992382      interface-state-change                     major
2023-06-01:00:40:39.040929      fib-updates                               minor
2023-06-01:00:40:39.041866      fib-updates                               minor
```

show sdwan appqoe

To view infrastructure statistics, NAT statistics, resource manager resources and statistics, TCP optimization status, and service chain status, use the **show sdwan appqoe** command in privileged EXEC mode.

show sdwan appqoe { **infra-statistics** | **nat-statistics** | **rm-statistics** | **ad-statistics** | **aoim-statistics** | **rm-resources** | **tcpopt status** | **service-chain status** | **libuinet-statistics** [**sppi** | **verbose**] }

Syntax Description

infra-statistics	Displays infra statistics
nat-statistics	Displays NAT statistics
rm-statistics	Displays resource manager status
ad-statistics	Displays the status for auto discovery of peer devices
aoim-statistics	Displays the statistics for one time exchange of information between peer devices
rm-resources	Displays resource manager resources
tcpopt status	Displays information about TCP optimization
service-chain status	Displays service chain status
libuinet-statistics sppi verbose	Displays libuinet statistics

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	Command introduced.

```
Device# show sdwan appqoe tcpopt status
=============================================================
                  TCP-OPT Status
=============================================================

Status
------
TCP OPT Operational State      : RUNNING
TCP Proxy Operational State    : RUNNING
```

```
Device#show sdwan appqoe nat-statistics
=============================================================
              NAT Statistics
=============================================================
 Insert Success      : 48975831
 Delete Success      : 48975823
 Duplicate Entries   : 19
 Allocation Failures : 0
 Port Alloc Success  : 0
 Port Alloc Failures : 0
 Port Free Success   : 0
 Port Free Failures  : 0
```

```
Device# show sdwan appqoe service-chain status
Service                   State
-------                   -----
SNORT Connection          UP
```

```
Device#  sdwan appqoe libuinet-statistics
=============================================================
              Libuinet Statistics
=============================================================
SPPI Statistics:
 Available Packets          : 1214696704
 Errored Available Packets  : 111235402
 Rx Packets                 : 1214696704
 Failed Rx Packets          : 0
 Tx Packets                 : 1124139791
 Tx Full Wait               : 0
 Failed Tx Packets          : 0
 PD Alloc Success           : 1226942851
 PD Alloc Failed            : 0
 PB Current Count           : 32768
 Pipe Disconnect            : 0

Vpath Statistics:
 Packets In                 : 1214696704
 Control Packets            : 250438
 Data Packets               : 1214446263
 Packets Dropped            : 351131
 Non-Vpath Packets          : 3
 Decaps                     : 1214446263
 Encaps                     : 1123889349
 Packets Out                : 1111643206
 Syn Packets                : 12248341
 Syn Drop Max PPS Reached   : 0
 IP Input Packets           : 1214095132
 IP Input Bytes             : 856784254349
 IP Output Packets          : 1111643202
```

```
 IP Output Bytes            : 917402419856
 Flow Info Allocs           : 12248341
 Flow Info Allocs Failed    : 0
 Flow Info Allocs Freed     : 12248339
 Rx Version Prob Packets    : 1
 Rx Control Packets         : 250437
 Rx Control Healthprobe Pkts: 250437
 ICMP incoming packet count: 0
 ICMP processing success: 0
 ICMP processing failures: 0
 Non-Syn nat lkup failed Pkts: 348691
 Nat lkup success for Syn Pkts: 248
 Vpath drops due to min threshhold: 0
 Flow delete notify TLV Pkts: 12246147
 Failed to allocate flow delete notify TLV Pkts: 0
 Failed to send flow delete notify TLV Pkts: 0
 Failed to create new connection: 2192
```

```
Device# show sdwan appqoe rm-resources
============================================================
              RM Resources
============================================================
RM Global Resources :
 Max Services Memory (KB)    : 1537040
 Available System Memory(KB) : 3074080
 Used Services Memory (KB)   : 228
 Used Services Memory (%)    : 0
 System Memory Status        : GREEN
 Num sessions Status         : GREEN
 Overall HTX health Status   : GREEN

Registered Service Resources :
TCP Resources:
 Max Sessions                : 40000
 Used Sessions               : 42
 Memory Per Session          : 128
SSL Resources:
 Max Sessions                : 40000
 Used Sessions               : 2
 Memory Per Session          : 50
```

```
Device# show sdwan appqoe ad-statistics

============================================================

              Auto-Discovery Statistics

============================================================

 Auto-Discovery Option Length Mismatch       : 0

 Auto-Discovery Option Version Mismatch      : 0

 Tcp Option Length Mismatch                  : 6

 AD Role set to NONE                         : 0

 [Edge] AD Negotiation Start                 : 96771

 [Edge] AD Negotiation Done                  : 93711

 [Edge] Rcvd SYN-ACK w/o AD options          : 0

 [Edge] AOIM sync Needed                     : 99
```

```
 [Core] AD Negotiation Start                 : 10375
 [Core] AD Negotiation Done                  : 10329
 [Core] Rcvd ACK w/o AD options              : 0
 [Core] AOIM sync Needed                     : 0
Device# show sdwan appqoe aoim-statistics
============================================================
              AOIM Statistics
============================================================
 Total Number Of Peer Syncs      : 1
 Current Number Of Peer Syncs in Progress      : 0
 Number Of Peer Re-Syncs Needed      : 1
 Total Passthrough Connections Due to Peer Version Mismatch   : 0
 AOIM DB Size (Bytes): 4194304

 LOCAL AO Statistics
----------------------------------------
 Number Of AOs      : 2
 AO             Version   Registered
 SSL             1.2        Y
 DRE             0.23       Y

 PEER Statistics
----------------------------------------
 Number Of Peers      : 1
 Peer ID: 203.203.203.11
 Peer Num AOs      : 2
 AO             Version   InCompatible
 SSL             1.2        N
 DRE             0.23       N
```

show sdwan appqoe dreopt

To view various DRE optimization statistics, use the **show sdwan appqoe dreopt** command in privileged EXEC mode.

show sdwan appqoe dreopt { **auto-bypass** | **crypt** | **status** [**detail**] }

Syntax Description

auto-bypass	Displays the auto-bypass details of DRE optimization.
crypt	Displays cache encryption status.
status	Displays DRE optimization status.
detail	(Optional) Displays a more detailed status of DRE optimization.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	This command was introduced.
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	This command was modified to include details of DRE profiles. This feature was introduced in Cisco IOS XE Catalyst SD-WAN Release 17.6.1a.

The following example shows the status of DRE optimization. To view the status in more detail, use the **show sdwan appqoe dreopt status detail** command.

```
Device# show sdwan appqoe dreopt status

DRE ID                                          : 52:54:dd:d0:e2:8d-0176814f0f66-93e0830d

DRE uptime                                      : 18:27:43

Health status                                   : GREEN

Health status change reason                     : None

Last health status change time                  : 18:25:29

Last health status notification sent time       : 1 second

DRE cache status                                : Active

Disk cache usage                                : 91%

Disk latency                                    : 16 ms

Active alarms:

  None
```

```
Configuration:

  Profile type                              : Default

  Maximum connections                       : 750

  Maximum fanout                            : 35

  Disk size                                 : 400 GB

  Memory size                               : 4096 MB

  CPU cores                                 : 1

  Disk encryption                           : ON
```

The following example shows how to view the auto-bypass status of DRE optimization.

```
Device# show sdwan appqoe dreopt auto-bypass

      Server IP   Port       State    DRE LAN BYTES    DRE WAN BYTES    DRE COMP   Last
Update   Entry Age
-------------------------------------------------------------------------------------------------

      10.0.0.1    9088       Monitor      48887002724      49401300299   0.000000
13:41:51   03:08:53
```

The following example shows how to view the cache encryption status for DRE.

```
Device# show sdwan appqoe dreopt crypt

Status: Success

Atempts: 1

1611503718:312238        DECRYPT REQ SENT

1611503718:318198        CRYPT SUCCESS

ENCRYPTION:

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

BLK NAME        :  No of Oper  | Success | Failure

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

SIGNATURE BLOCK |     210404     210404          0

SEGMENT BLOCK   |     789411     789411          0

SECTION BLOCKS  |      49363      49363          0

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

DECRYPTION:

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

BLK NAME        :  No of Oper  | Success | Failure

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

SIGNATURE BLOCK |     188616     188616          0
```

```
SEGMENT BLOCK   |          1          1          0

SECTION BLOCKS  |     366342     366342          0

-------------------------------------------------
```

Following is the sample output from the **show sdwan appqoe dreopt status** command. This example shows the details of the DRE profile applied.

```
Device# show sdwan appqoe dreopt status
DRE ID                                          : 52:54:dd:e5:58:5a-01791db8c691-c5b3336c
DRE uptime                                      : 20:58:23
Health status                                   : GREEN
Health status change reason                     : None
Last health status change time                  : 19:40:37
Last health status notification sent time       : 1 second
DRE cache status                                : Active
Disk cache usage                                : 0%
Disk latency                                    : 0 ms
Active alarms:
  None
Configuration:
  Profile type                              : S
  Maximum connections                       : 750
  Maximum fanout                            : 35
  Disk size                                 : 60 GB
  Memory size                               : 2048 MB
  CPU cores                                 : 1
  Disk encryption
```

show sdwan appqoe dreopt statistics

To view DRE optimization statistics, use the **show sdwan appqoe dreopt statistics** command in privileged EXEC mode.

show sdwan appqoe dreopt statistics [**detail** | **peer** [**detail** | **peer** *peer-ip* | **peer-no** *peer-id*]]

Syntax Description

detail	(Optional) Displays detailed DRE optimization statistics.
peer *peer-ip*	(Optional) Displays DREOPT peer details.
peer-no *peer-id*	(Optional) Displays DRE optimization details for peer-no.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command introduced.

The following information show how to view DRE optimization statistics.

```
Device# show sdwan appqoe dreopt statistics

Total connections                 : 3714
```

```
Max concurrent connections         : 552
Current active connections         : 0
Total connection resets            : 1081
Total original bytes               : 360 GB
Total optimized bytes              : 164 GB
Overall reduction ratio            : 54%
Disk size used                     : 91%
Cache details:
  Cache status                       : Active
  Cache Size                         : 407098 MB
  Cache used                         : 91%
  Oldest data in cache               : 03:02:07:55
  Replaced(last hour): size          : 0 MB
```

The following example shows DRE optimization statistics for a peer device.

```
Device# show sdwan appqoe dreopt statistics peer 209.165.201.1

  Peer No.  System IP          Hostname    Active connections    Cummulative connections
-------------------------------------------------------------------------------------------

         0  209.165.201.1       dreopt              0                       3714
```

show sdwan appqoe error recent

To view details of recent AppQoE errors, use the **show sdwan appqoe error recent** command in privileged EXEC mode.

show sdwan appqoe error recent

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	This command was introduced.

Example

The following is sample output from the **show sdwan appqoe error recent**

```
Device# show sdwan appqoe error recent

Appqoe Statistics Recent

------------------------
```

Label	Current value	Value(30 sec bfr)	Value(60 sec bfr)
RM TCP used sessions	20702	20026	21005
RM SSL used sessions	19376	18528	18824
RM health status change to yellow	47	47	47
RM health status change to green	47	47	47
RM TCP session allocated	28412162	28406875	28402421
RM TCP session freed	28391460	28386849	28381416
RM SSL session allocated	28412144	28406857	28402403
RM SSL session freed	28392768	28388329	28383579
TCP number of connections	27597418	27592148	27588196
TCP number of flows created	28412162	28406875	28402421
TCP number of flows deleted	28389923	28385898	28381006
TCP number of current connections	19687	19026	20504
TCP failed connections	813651	813649	813646
TCP syncache added	28411831	28406269	28402046
vPath drop due to pps	578	578	578
vPath new connection failed	11757	11757	11757
BBR Active connections	38108	35305	38252
BBR sendmap allcation failed	0	0	0
SPPI available packets	3898784336	3896241285	3893452077
SPPI failed received packets	0	0	0
SPPI failed transmitted packets	0	0	0
SPPI pipe disconnected	0	0	0
HPUT SYS TIMER callout deleted	0	0	0
HPUT HPTS TIMER callout deleted	0	0	0
HPUT SYS TIMER timer deleted	111372027	111351614	111325475
HPUT HPTS TIMER timer deleted	11873674	11873666	11873651
HPUT SYS TIMER node is empty	0	0	0
HPUT HPTS TIMER node is empty	459711	459708	459699

```
Untrusted Certificate              0                  0                  0
Unable to get Proxy certificate    954                954                954
Expired Certificate                0                  0                  0
OCSP Cert Verification Failure     0                  0                  0
Endpoint Alert                     0                  0                  0
FIN/RST Received during handshake  172444             172444             172444
Session Alloc Failures             0                  0                  0
C2S WCAPI DENY packet              0                  0                  0
S2C WCAPI DENY packet              0                  0                  0
```

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

Table 100: show sdwan appqoe error recent Field Descriptions

Field	Description
RM TCP used sessions	The number of resource manager sessions used by TCP proxy
RM SSL used sessions	The number of resource manager sessions used by SSL proxy
RM health status change to yellow	The number of times the status of the resource manager changed to yellow
RM health status change to green	The number of times the status of the resource manager changed to green
RM TCP session allocated	The number of resource manager sessions allocated by TCP proxy
RM TCP session freed	The number of resource manager sessions freed by TCP proxy
RM SSL session allocated	The number of resource manager sessions allocated by SSL proxy
RM SSL session freed	The number of resource manager sessions freed by SSL proxy
TCP number of connections	The total number of TCP connections
TCP number of flows created	The total number of TCP flows created
TCP number of flows deleted	The total number of TCP flows deleted
TCP number of current connections	The total number of current TCP connections
TCP syncache added	The total number of SYN cache entries

Field	Description
vPath drop due to pps	The total number of transport channel SYN entries dropped because the packet-per-second limit is reached
vPath new connection failed	The total number of new transport channel connections that failed
BBR Active Connections	The total number of active connections for Bottleneck Bandwidth and Round-trip (BBR) propagation
BBR sendmap allocation failed	The total numbers of BBR total send map allocation failures
SPPI available packets	Total packets available for Service Plane Packet Interface (SPPI)
SPPI pipe disconnected	SPPI pipe is disconnected
SPPI failed received packets	SPPI failed to receive packets
SPPI failed transmit packets	SPPI failed to transmit packets
HPUT SYS TIMER callout deleted	System timer callout was deleted
HPUT HPTS TIMER callout deleted	The high-precision timers (HPTS) callout was deleted
HPUT SYS TIMER timer deleted	The system timer was deleted
HPUT HPTS TIMER timer deleted	The HPTS timer was deleted
HPUT SYS TIMER node is empty	The system timer node is empty
HPUT HPTS TIMER node is empty	The HPTS timer node is empty
Untrusted Certificate	Total number of SSL sessions dropped because of untrusted certificates
Unable to get Proxy certificate	The total number of sessions dropped because the SSL proxy certificate couldn't be retrieved
Expired Certificate	The total number of SSL sessions dropped due to expired certificates
OCSP Cert Verification Failure	The number of failures because the OSCP certificate verification failed
Endpoint Alert	The number of SSL proxy sessions dropped because of endpoint alerts
FIN/RST Received during handshake	SSL was dropped because TCP connection was closed
Session Alloc Failures	SSL proxy could not allocate sessions
C2S WCAPI DENY packet	The SSL client to server packet was denied

Field	Description
S2C WCAPI DENY packet	The SSL server to client packet was denied

show sdwan appqoe flow closed all

To display the summary of AppQoE expired flows on a device, use the **show sdwan appqoe flow closed all** command in privileged EXEC mode.

show sdwan appqoe flow closed all

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This command was introduced.

Examples

The following sample output displays the summary of AppQoE expired flows.

```
Device# show sdwan appqoe flow closed all
Current Historical Optimized Flows: 16

Optimized Flows
---------------
T:TCP, S:SSL, U:UTD, D:DRE, H:HTTP
RR: DRE Reduction Ratio

Flow ID      VPN  Source IP:Port        Destination IP:Port   Service  RR%
22977217840  1    30.1.50.2:34940       30.1.51.2:80          T        -
13598953631  1    30.1.50.2:34936       30.1.51.2:80          T        -
17348519476  1    30.1.50.2:34938       30.1.51.2:80          T        -
11495519740  1    30.1.50.2:34934       30.1.51.2:80          T        -
29497270355  1    30.1.50.2:34942       30.1.51.2:80          T        -
32442796471  1    30.1.50.2:34944       30.1.51.2:80          T        -
34529471700  1    30.1.50.2:34946       30.1.51.2:80          T        -
39369775743  1    30.1.50.2:34948       30.1.51.2:80          T        -
46676987507  1    30.1.50.2:34950       30.1.51.2:80          T        -
8568888344   1    30.1.50.2:34932       30.1.51.2:80          T        -
63035789628  1    30.1.50.2:34958       30.1.51.2:80          T        -
48746883856  1    30.1.50.2:34952       30.1.51.2:80          T        -
51709149940  1    30.1.50.2:34954       30.1.51.2:80          T        -
58212427671  1    30.1.50.2:34956       30.1.51.2:80          T        -
66801636855  1    30.1.50.2:34960       30.1.51.2:80          T        -
68888309908  1    30.1.50.2:34962       30.1.51.2:80          T        -
```

Related Commands

Command	Description
show sdwan appqoe flow closed flow-id *flow-id*	Displays AppQoE expired flow details for a single specific flow.

Command	Description
show sdwan appqoe flow flow-id *flow-id*	Displays the details of a single specific flow.
show sdwan appqoe flow vpn-id *vpn-id* **server-port** *server-port*	Displays the flows for a specific VPN on a device.

show sdwan appqoe flow closed flow-id

To display AppQoE expired flow details for a signle specific flow on a device, use the **show sdwan appqoe flow closed flow-id** command in privileged EXEC mode.

show sdwan appqoe flow closed flow-id *flow-id*

Supported Parameters

flow-id	Specify a flow id.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This command was introduced.

Examples

The following sample output displays the AppQoE expired flow details for a signle specific flow.

```
Device# show sdwan appqoe flow closed flow-id 66801636855
Flow ID: 66801636855

VPN: 1  APP: 0 [Client 30.1.50.2:34960 - Server 30.1.51.2:80]

TCP stats
---------
Client Bytes Received   : 139
Client Bytes Sent       : 10486028
Server Bytes Received   : 10486028
Server Bytes Sent       : 139

Client Bytes sent to SSL: 0
Server Bytes sent to SSL: 0

C2S HTX to DRE Bytes    : 0
C2S HTX to DRE Pkts     : 0
S2C HTX to DRE Bytes    : 0
S2C HTX to DRE Pkts     : 0
C2S DRE to HTX Bytes    : 0
C2S DRE to HTX Pkts     : 0
S2C DRE to HTX Bytes    : 0
```

```
S2C DRE to HTX Pkts     : 0

C2S HTX to HTTP Bytes   : 0
C2S HTX to HTTP Pkts    : 0
S2C HTX to HTTP Bytes   : 0
S2C HTX to HTTP Pkts    : 0
C2S HTTP to HTX Bytes   : 0
C2S HTTP to HTX Pkts    : 0
S2C HTTP to HTX Bytes   : 0
S2C HTTP to HTX Pkts    : 0

C2S SVC Bytes to SSL    : 0
S2C SVC Bytes to SSL    : 0
C2S SSL to TCP Tx Pkts  : 0
C2S SSL to TCP Tx Bytes : 0
S2C SSL to TCP Tx Pkts  : 0
S2C SSL to TCP Tx Bytes : 0

C2S TCP Tx Pkts Success : 1
C2S TCP Tx Pkts Failed  : 0
S2C TCP Tx Pkts Success : 7515
S2C TCP Tx Pkts Failed  : 0

TCP Client IP TOS       : 0x28
TCP Server IP TOS       : 0x28
TCP Client Rx Pause     : 0x1
TCP Server Rx Pause     : 0x1
TCP Client Tx Pause     : 0x0
TCP Server Tx Pause     : 0x0
Client Flow Pause State : 0x0
Server Flow Pause State : 0x0
Client Flow Control     : 0x0
Server Flow Control     : 0x0
Snort close sent : 0x0
Snort init close handled: 0x0
TCP Flow Bytes Consumed[C2S][Og] : 0
TCP Flow Bytes Consumed[C2S][Tm] : 0
TCP Flow Bytes Consumed[S2C][Og] : 0
TCP Flow Bytes Consumed[S2C][Tm] : 0
TCP Client Close Done   : 0x1
TCP Server Close Done   : 0x1
TCP Client FIN Rcvd     : 0x1
TCP Server FIN Rcvd     : 0x1
TCP Client RST Rcvd     : 0x0
TCP Server RST Rcvd     : 0x0
TCP Client FIN Sent     : 0x1
TCP Server FIN Sent     : 0x1
Flow Cleanup State      : 0x7
TCP Flow Events
   1. time:2252.112679   ::   Event:TCPPROXY_EVT_FLOW_CREATED
   2. time:2252.112697   ::   Event:TCPPROXY_EVT_AD_RX_SYN_WITHOUT_OPTIONS
   3. time:2252.112725   ::   Event:TCPPROXY_EVT_SYNCACHE_ADDED
   4. time:2252.112736   ::   Event:TCPPROXY_EVT_AD_TX_EDGE_SYNACK_NO_OPTIONS
   5. time:2252.113091   ::   Event:TCPPROXY_EVT_AD_RX_EDGE_ACK
   6. time:2252.113180   ::   Event:TCPPROXY_EVT_ACCEPT_DONE
   7. time:2252.113286   ::   Event:TCPPROXY_EVT_AD_TX_EDGE_SYN
   8. time:2252.113292   ::   Event:TCPPROXY_EVT_CONNECT_START
   9. time:2253.113338   ::   Event:TCPPROXY_EVT_AD_TX_EDGE_SYN
  10. time:2254.122111   ::   Event:TCPPROXY_EVT_AD_RX_EDGE_SYNACK_WITH_OPTIONS
  11. time:2254.122209   ::   Event:TCPPROXY_EVT_CONNECT_DONE
  12. time:2254.122230   ::   Event:TCPPROXY_EVT_DATA_ENABLED_SUCCESS
  13. time:2254.122281   ::   Event:TCPPROXY_EVT_AD_TX_EDGE_ACK
  14. time:2254.122299   ::   Event:TCPPROXY_EVT_AD_TX_EDGE_ACK
  15. time:2757.323156   ::   Event:TCPPROXY_EVT_FIN_RCVD_CLIENT_FD_C2S
```

```
 16. time:2757.323164   ::   Event:TCPPROXY_EVT_FIN_SENT_SERVER_FD_C2S
 17. time:2757.330780   ::   Event:TCPPROXY_EVT_FIN_RCVD_SERVER_FD_S2C
 18. time:2757.330781   ::   Event:TCPPROXY_EVT_SERVER_TCP_CLOSED
 19. time:2757.330781   ::   Event:TCPPROXY_EVT_ENABLE_RX_SOCK_ON_STACK_CLOSED_SERVER
 20. time:2757.330790   ::   Event:TCPPROXY_EVT_FIN_SENT_CLIENT_FD_S2C
 21. time:2757.330807   ::   Event:TCPPROXY_EVT_CLOSE_CLIENT_FD_S2C
 22. time:2757.330807   ::   Event:TCPPROXY_EVT_CLOSE_SERVER_FD_C2S
 23. time:2757.330807   ::   Event:TCPPROXY_EVT_PROXY_CLOSE
 24. time:2757.330962   ::   Event:TCPPROXY_EVT_CLIENT_TCP_CLOSED
 25. time:2757.330963   ::   Event:TCPPROXY_EVT_ALL_TCP_CLOSED_CLEANUP
 26. time:2763.084297   ::   Event:TCPPROXY_EVT_CLEANUP_COMPLETE


TCP BBR Client Statistics:
 BBR States Transition
     STARTUP To DRAIN State     : 0
     STARTUP To PROBEBW State   : 1
     STARTUP To PROBERTT State  : 0
     DRAIN To PROBEBW State     : 0
     PROBEBW To PROBERTT State  : 21
     PROBERTT To STARTUP State  : 0
     PROBERTT To PROBEBW State  : 21
     IDLEEXIT To PROBEBW State  : 0
 HPTS Timer Started
     Wrong Timer                : 0
     Persistent Timeout         : 0
     Keepalive Timeout          : 0
     Connection Initialization  : 0
     BBR do segment unlock1     : 1
     BBR do segment unlock2     : 0
     PACE Segment               : 20828
     BBR output wtime error msg size: 0
     BBR output wtime default   : 0
     BBR do wtime error nonufs  : 6
 HPTS Timer Stopped
     Wrong Timer                : 0
     Cancel Timer               : 6008
     Persistent Mode Exit       : 0
     BBR Do Segment Unlock      : 0
     Packets needs to be paced  : 7388
     Exempt early               : 0
     Delay exceed               : 91
     Connection Closed          : 0
 Pacing Delay (in us)
     Equals 0           : 0
     1 to 5             : 7341
     6 to 10            : 15
     11 to 20           : 63
     21 to 50           : 15
     50 to 100          : 4
     101 to 500         : 0
     501 to 1000        : 36
     Greater than 1000  : 13361
 RTT (in ms)
     Less than 1       : 2009
     Equals 1          : 2
     1 To 50           : 4297
     51 To 100         : 0
     101 To 150        : 0
     151 To 200        : 0
     Greater than 200  : 0
 Bandwidth
     Less Than 1KBps     : 2
     1KBps To 250KBps    : 5618
```

```
    251KBps To 500KBps  : 1
    500KBps To 1MBps    : 0
    1MBps To 2MBps      : 2
    2MBps To 5MBps      : 257
    5MBps To 10MBps     : 194
    Greater Than 10MBps : 234
 BBR Output Bytes              : 10486028
 TCP Segments Lost             : 0
 TCP Segment Sent              : 7820
 Retransmitted Segments        : 0
 Conn. drop due to no progress : 0
 TCP Segment Sent through HPTS : 7355
 Max Send Buffer Reached       : 20830
 Max Send Congestion Window    : 353998
 Current TCP Send Window       : 821632

HPTS Statistics:
 Timer Expired Early         : 0
 Delay in Timer Expiry       : 7441
 Callout Scheduled           : 0
 Lasttick is gt current tick : 0
 Maxticks Overflow           : 0
 Timer WakeUp Immediately    : 0
 Inp Added back to same slot : 0
 Distance To Travel Overflow : 0
 Available On Wheel Overflow : 0
 Available On Wheel lt Pacer : 0
 HPTS Is Hopelessly Behind   : 0
 HPTS Is Stuck In Loop       : 0
 HPTS Is Back On Sleep       : 0
 HPTS Wheel Wrapped          : 0
 HPTS Wheel Time Exceeded    : 0
 Forced close from FIN_WAIT_2  : 0

TCP BBR Server Statistics:
 BBR States Transition
    STARTUP To DRAIN State     : 0
    STARTUP To PROBEBW State   : 0
    STARTUP To PROBERTT State  : 0
    DRAIN To PROBEBW State     : 0
    PROBEBW To PROBERTT State  : 0
    PROBERTT To STARTUP State  : 0
    PROBERTT To PROBEBW State  : 0
    IDLEEXIT To PROBEBW State  : 0
 HPTS Timer Started
    Wrong Timer                 : 0
    Persistent Timeout          : 0
    Keepalive Timeout           : 0
    Connection Initialization   : 0
    BBR do segment unlock1      : 3755
    BBR do segment unlock2      : 0
    PACE Segment                : 3
    BBR output wtime error msg size: 0
    BBR output wtime default    : 0
    BBR do wtime error nonufs   : 4203
 HPTS Timer Stopped
    Wrong Timer               : 0
    Cancel Timer              : 3757
    Persistent Mode Exit      : 0
    BBR Do Segment Unlock     : 0
    Packets needs to be paced  : 4039
    Exempt early              : 0
    Delay exceed              : 0
    Connection Closed         : 0
```

```
 Pacing Delay (in us)
     Equals 0           : 0
     1 to 5             : 0
     6 to 10            : 0
     11 to 20           : 0
     21 to 50           : 0
     50 to 100          : 1
     101 to 500         : 0
     501 to 1000        : 0
     Greater than 1000  : 7958
 RTT (in ms)
     Less than 1       : 0
     Equals 1          : 0
     1 To 50           : 1
     51 To 100         : 0
     101 To 150        : 0
     151 To 200        : 0
     Greater than 200  : 448
 Bandwidth
     Less Than 1KBps     : 449
     1KBps To 250KBps    : 0
     251KBps To 500KBps  : 0
     500KBps To 1MBps    : 0
     1MBps To 2MBps      : 0
     2MBps To 5MBps      : 0
     5MBps To 10MBps     : 0
     Greater Than 10MBps : 0
 BBR Output Bytes              : 139
 TCP Segments Lost             : 0
 TCP Segment Sent              : 4204
 Retransmitted Segments        : 0
 Conn. drop due to no progress : 0
 TCP Segment Sent through HPTS : 163
 Max Send Buffer Reached       : 4204
 Max Send Congestion Window    : 1073725440
 Current TCP Send Window       : 0

HPTS Statistics:
 Timer Expired Early         : 0
 Delay in Timer Expiry       : 1
 Callout Scheduled           : 0
 Lasttick is gt current tick : 0
 Maxticks Overflow           : 0
 Timer WakeUp Immediately    : 0
 Inp Added back to same slot : 0
 Distance To Travel Overflow : 0
 Available On Wheel Overflow : 0
 Available On Wheel lt Pacer : 0
 HPTS Is Hopelessly Behind   : 0
 HPTS Is Stuck In Loop       : 0
 HPTS Is Back On Sleep       : 0
 HPTS Wheel Wrapped          : 0
 HPTS Wheel Time Exceeded    : 0
 Forced close from FIN_WAIT_2  : 0
```

Related Commands

Command	Description
show sdwan appqoe flow closed all	Displays the summary of AppQoE expired flows on a device.

Command	Description
show sdwan appqoe flow flow-id *flow-id*	Displays the details of a single specific flow.
show sdwan appqoe flow vpn-id *vpn-id* **server-port** *server-port*	Displays the flows for a specific VPN on a device.

show sdwan appqoe flow flow-id

To display the details for a single specific flow, use the **show sdwan appqoe flow flow-id** command in privileged EXEC mode.

show sdwan appqoe flow flow-id *flow-id*

Supported Parameters

flow-id	Specify a flow id.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This command was introduced.

Examples

The following sample output displays the details for a single specific flow.

```
Device# show sdwan appqoe flow flow-id 68888309908
Flow ID: 68888309908

VPN: 1  APP: 0 [Client 30.1.50.2:34962 - Server 30.1.51.2:80]

TCP stats
---------
Client Bytes Received   : 139
Client Bytes Sent       : 2625440
Server Bytes Received   : 2625440
Server Bytes Sent       : 139

Client Bytes sent to SSL: 0
Server Bytes sent to SSL: 0

C2S HTX to DRE Bytes    : 0
C2S HTX to DRE Pkts     : 0
S2C HTX to DRE Bytes    : 0
S2C HTX to DRE Pkts     : 0
C2S DRE to HTX Bytes    : 0
C2S DRE to HTX Pkts     : 0
S2C DRE to HTX Bytes    : 0
```

```
S2C DRE to HTX Pkts     : 0

C2S HTX to HTTP Bytes   : 0
C2S HTX to HTTP Pkts    : 0
S2C HTX to HTTP Bytes   : 0
S2C HTX to HTTP Pkts    : 0
C2S HTTP to HTX Bytes   : 0
C2S HTTP to HTX Pkts    : 0
S2C HTTP to HTX Bytes   : 0
S2C HTTP to HTX Pkts    : 0

C2S SVC Bytes to SSL    : 0
S2C SVC Bytes to SSL    : 0
C2S SSL to TCP Tx Pkts  : 0
C2S SSL to TCP Tx Bytes : 0
S2C SSL to TCP Tx Pkts  : 0
S2C SSL to TCP Tx Bytes : 0

C2S TCP Tx Pkts Success : 1
C2S TCP Tx Pkts Failed  : 0
S2C TCP Tx Pkts Success : 1912
S2C TCP Tx Pkts Failed  : 0
TCP Client IP TOS       : 0x28
TCP Server IP TOS       : 0x28
TCP Client Rx Pause     : 0x0
TCP Server Rx Pause     : 0x0
TCP Client Tx Enabled   : 0x0
TCP Server Tx Enabled   : 0x0
Client Flow Pause State : 0x0
Server Flow Pause State : 0x0
Client Flow Control     : 0x0
Server Flow Control     : 0x0
Snort close sent : 0x0
Snort init close handled: 0x0
TCP Flow Bytes Consumed[C2S][Og] : 0
TCP Flow Bytes Consumed[C2S][Tm] : 0
TCP Flow Bytes Consumed[S2C][Og] : 0
TCP Flow Bytes Consumed[S2C][Tm] : 0
TCP Client Close Done   : 0x0
TCP Server Close Done   : 0x0
TCP Client FIN Rcvd     : 0x0
TCP Server FIN Rcvd     : 0x0
TCP Client RST Rcvd     : 0x0
TCP Server RST Rcvd     : 0x0
TCP Client FIN Sent     : 0x0
TCP Server FIN Sent     : 0x0
Flow Cleanup State      : 0x0
AD State            : AD_STATE_TX_ACK
AD Nego Role        : AD_ROLE_EDGE
AD peer ID          : 0xc0a80d01
AD configured Policy: 0x8
AD derived Policy   : 0x8
AD peer Policy      : 0x0
AD applied Policy   : 0x0
AOIM sync Needed    : No
Client Resume Enq Count : 0
Client Resume Enq Ign   : 0
Client Resume Process   : 0
Client Resume Process Ign : 0
Server Resume Enq Count : 0
Server Resume Enq Ign   : 0
Server Resume Process   : 0
Server Resume Process Ign : 0
DRE C2S Paused Count        : 0
```

```
DRE C2S Resumed Sent Count  : 0
DRE C2S Resume Recv Count   : 0
DRE S2C Paused Count        : 0
DRE S2C Resume Sent Count   : 0
DRE S2C Resume Recv Count   : 0
HTTP C2S Paused Count        : 0
HTTP C2S Resumed Sent Count  : 0
HTTP C2S Resume Recv Count   : 0
HTTP S2C Paused Count        : 0
HTTP S2C Resume Sent Count   : 0
HTTP S2C Resume Recv Count   : 0
SSL RD Pause/fail C2S Orig  : 0/0
SSL RD Resume Notify C2S Og : 0
SSL RD Resume C2S Orig      : 0
SSL RD Pause/fail C2S Term  : 0/0
SSL RD Resume Notify C2S Tm : 0
SSL RD Resume C2S Term      : 0
SSL RD Pause/fail S2C Orig  : 0/0
SSL RD Resume Notify S2C Og : 0
SSL RD Resume S2C Orig      : 0
SSL RD Pause/fail S2C Term  : 0/0
SSL RD Resume Notify S2C Tm : 0
SSL RD Resume S2C Term      : 0
SSL Proxy Client Bytes [C2S]: 0
SSL Proxy Client Bytes [S2C]: 0
SSL Proxy Server Bytes [C2S]: 0
SSL Proxy Server Bytes [S2C]: 0
Rx Client Queue Length      : 0
Rx Server Queue Length      : 0
SVC-to-Client Queue Length  : 0
SVC-to-Server Queue Length  : 0
TCP Flow Events
   1. time:2781.598055   ::   Event:TCPPROXY_EVT_FLOW_CREATED
   2. time:2781.598077   ::   Event:TCPPROXY_EVT_AD_RX_SYN_WITHOUT_OPTIONS
   3. time:2781.598128   ::   Event:TCPPROXY_EVT_SYNCACHE_ADDED
   4. time:2781.598145   ::   Event:TCPPROXY_EVT_AD_TX_EDGE_SYNACK_NO_OPTIONS
   5. time:2781.598473   ::   Event:TCPPROXY_EVT_AD_RX_EDGE_ACK
   6. time:2781.598621   ::   Event:TCPPROXY_EVT_ACCEPT_DONE
   7. time:2781.598739   ::   Event:TCPPROXY_EVT_AD_TX_EDGE_SYN
   8. time:2781.598747   ::   Event:TCPPROXY_EVT_CONNECT_START
   9. time:2781.599958   ::   Event:TCPPROXY_EVT_AD_RX_EDGE_SYNACK_WITH_OPTIONS
  10. time:2781.599984   ::   Event:TCPPROXY_EVT_AD_TX_EDGE_ACK
  11. time:2781.599985   ::   Event:TCPPROXY_EVT_CONNECT_DONE
  12. time:2781.600006   ::   Event:TCPPROXY_EVT_DATA_ENABLED_SUCCESS
  13. time:2781.600061   ::   Event:TCPPROXY_EVT_AD_TX_EDGE_ACK


TCP BBR Client Statistics:
 BBR States Transition
     STARTUP To DRAIN State     : 0
     STARTUP To PROBEBW State   : 1
     STARTUP To PROBERTT State  : 0
     DRAIN To PROBEBW State     : 0
     PROBEBW To PROBERTT State  : 1
     PROBERTT To STARTUP State  : 0
     PROBERTT To PROBEBW State  : 1
     IDLEEXIT To PROBEBW State  : 0
 HPTS Timer Started
     Wrong Timer                : 0
     Persistent Timeout         : 0
     Keepalive Timeout          : 0
     Connection Initialization  : 0
     BBR do segment unlock1     : 1
     BBR do segment unlock2     : 0
```

```
    PACE Segment                : 4752
    BBR output wtime error msg size: 0
    BBR output wtime default    : 0
    BBR do wtime error nonufs   : 7
 HPTS Timer Stopped
    Wrong Timer                 : 0
    Cancel Timer                : 984
    Persistent Mode Exit        : 0
    BBR Do Segment Unlock       : 0
    Packets needs to be paced   : 1881
    Exempt early                : 0
    Delay exceed                : 17
    Connection Closed           : 0
 Pacing Delay (in us)
    Equals 0           : 0
    1 to 5             : 1885
    6 to 10            : 5
    11 to 20           : 1
    21 to 50           : 2
    50 to 100          : 1
    101 to 500         : 0
    501 to 1000        : 7
    Greater than 1000  : 2859
 RTT (in ms)
    Less than 1       : 1051
    Equals 1          : 1
    1 To 50           : 0
    51 To 100         : 0
    101 To 150        : 0
    151 To 200        : 0
    Greater than 200  : 0
 Bandwidth
    Less Than 1KBps     : 1
    1KBps To 250KBps    : 889
    251KBps To 500KBps  : 0
    500KBps To 1MBps    : 0
    1MBps To 2MBps      : 0
    2MBps To 5MBps      : 39
    5MBps To 10MBps     : 64
    Greater Than 10MBps : 59
 BBR Output Bytes              : 2628130
 TCP Segments Lost             : 0
 TCP Segment Sent              : 1958
 Retransmitted Segments        : 0
 Conn. drop due to no progress : 0
 TCP Segment Sent through HPTS : 1877
 Max Send Buffer Reached       : 4752
 Max Send Congestion Window    : 196370
 Current TCP Send Window       : 321024

HPTS Statistics:
 Timer Expired Early         : 0
 Delay in Timer Expiry       : 1894
 Callout Scheduled           : 0
 Lasttick is gt current tick : 0
 Maxticks Overflow           : 0
 Timer WakeUp Immediately    : 0
 Inp Added back to same slot : 0
 Distance To Travel Overflow : 0
 Available On Wheel Overflow : 0
 Available On Wheel lt Pacer : 0
 HPTS Is Hopelessly Behind   : 0
 HPTS Is Stuck In Loop       : 0
 HPTS Is Back On Sleep       : 0
```

```
 HPTS Wheel Wrapped          : 0
 HPTS Wheel Time Exceeded    : 0
 Forced close from FIN_WAIT_2  : 0

TCP BBR Server Statistics:
 BBR States Transition
     STARTUP To DRAIN State     : 0
     STARTUP To PROBEBW State   : 0
     STARTUP To PROBERTT State  : 0
     DRAIN To PROBEBW State     : 0
     PROBEBW To PROBERTT State  : 0
     PROBERTT To STARTUP State  : 0
     PROBERTT To PROBEBW State  : 0
     IDLEEXIT To PROBEBW State  : 0
 HPTS Timer Started
     Wrong Timer                 : 0
     Persistent Timeout          : 0
     Keepalive Timeout           : 0
     Connection Initialization   : 0
     BBR do segment unlock1      : 976
     BBR do segment unlock2      : 0
     PACE Segment                : 3
     BBR output wtime error msg size: 0
     BBR output wtime default    : 0
     BBR do wtime error nonufs   : 979
 HPTS Timer Stopped
     Wrong Timer                : 0
     Cancel Timer               : 978
     Persistent Mode Exit       : 0
     BBR Do Segment Unlock      : 0
     Packets needs to be paced  : 978
     Exempt early               : 0
     Delay exceed               : 0
     Connection Closed          : 0
 Pacing Delay (in us)
     Equals 0           : 0
     1 to 5             : 1
     6 to 10            : 0
     11 to 20           : 0
     21 to 50           : 0
     50 to 100          : 0
     101 to 500         : 0
     501 to 1000        : 0
     Greater than 1000  : 1958
 RTT (in ms)
     Less than 1       : 0
     Equals 1          : 0
     1 To 50           : 2
     51 To 100         : 0
     101 To 150        : 0
     151 To 200        : 0
     Greater than 200  : 0
 Bandwidth
     Less Than 1KBps     : 1
     1KBps To 250KBps    : 1
     251KBps To 500KBps  : 0
     500KBps To 1MBps    : 0
     1MBps To 2MBps      : 0
     2MBps To 5MBps      : 0
     5MBps To 10MBps     : 0
     Greater Than 10MBps : 0
 BBR Output Bytes              : 139
 TCP Segments Lost             : 0
 TCP Segment Sent              : 980
```

```
 Retransmitted Segments        : 0
 Conn. drop due to no progress : 0
 TCP Segment Sent through HPTS : 1
 Max Send Buffer Reached       : 982
 Max Send Congestion Window    : 1073725440
 Current TCP Send Window       : 0

HPTS Statistics:
 Timer Expired Early         : 0
 Delay in Timer Expiry       : 1
 Callout Scheduled           : 0
 Lasttick is gt current tick : 0
 Maxticks Overflow           : 0
 Timer WakeUp Immediately    : 0
 Inp Added back to same slot : 0
 Distance To Travel Overflow : 0
 Available On Wheel Overflow : 0
 Available On Wheel lt Pacer : 0
 HPTS Is Hopelessly Behind   : 0
 HPTS Is Stuck In Loop       : 0
 HPTS Is Back On Sleep       : 0
 HPTS Wheel Wrapped          : 0
 HPTS Wheel Time Exceeded    : 0
 Forced close from FIN_WAIT_2  : 0
```

Related Commands

Command	Description
show sdwan appqoe flow closed all	Displays the summary of AppQoE expired flows on a device.
show sdwan appqoe flow closed flow-id *flow-id*	display AppQoE expired flow details for a signle specific flow on a device.
show sdwan appqoe flow vpn-id *vpn-id* **server-port** *server-port*	Displays the flows for a specific VPN on a device.

show sdwan appqoe flow vpn-id

To display flows for a specific VPN on a device, use the **show sdwan appqoe flow vpn-id** command in privileged EXEC mode.

show sdwan appqoe flow vpn-id *vpn-id* **server-port** *server-port*

Supported Parameters

vpn-id	Specify a vpn id.
server-port	Specify a server port number.

Command Default

None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This command was introduced.

Examples

The following sample output displays flows for a specific VPN.

```
Device# show sdwan appqoe flow closed vpn-id 1 server-port 443
Current Historical Optimized Flows: 101

Optimized Flows
---------------
T:TCP, S:SSL, U:UTD, D:DRE, H:HTTP
RR: DRE Reduction Ratio

Flow ID          VPN Source IP:Port Destination IP:Port Service RR%
53486969779402663 1  11.0.0.5:50621 23.0.0.7:443        TDS 99
53488479953969085 1  11.0.0.5:52664 23.0.0.72:443       T-
53484184343020025 1  11.0.0.7:45862 23.0.0.14:443       TDS 99
53486924218325306 1  11.0.0.7:50518 23.0.0.70:443       TDS 99
```

Related Commands

Command	Description
show sdwan appqoe flow closed flow-id *flow-id*	Displays AppQoE expired flow details on a device.
show sdwan appqoe flow flow-id *flow-id*	Displays AppQoE Active flow details on a device.
show sdwan appqoe flow closed all	Displays the summary of AppQoE expired flows on a device.

show sdwan appqoe status

To view the status of various AppQoE modules, use the **show sdwan appqoe status** command in privileged EXEC mode.

show sdwan appqoe status

This command has no keywords or arguments.

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	This command was introduced.

Example

The following is sample output from the **show sdwan appqoe status** command.

```
Device# show sdwan appqoe status

APPQOE Status : GREEN

Service Status:

  SSLPROXY : GREEN

  TCPPROXY : GREEN

  SERVICE CHAIN : GREEN

  RESOURCE MANAGER : GREEN
```

show sdwan app-fwd cflowd collector

To display information about the configured cflowd collectors on Cisco IOS XE Catalyst SD-WAN devices, use the **show sdwan app-fwd cflowd collector** command in privileged exec mode.

show sdwan app-fwd cflowd collector

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Privileged exec (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Cflowd monitors traffic flowing through Cisco IOS XE Catalyst SD-WAN devices in the overlay network and exports flow information to a collector, where it can be processed by an IPFIX analyzer. A flow-visibility policy must be enabled to see output from this command. This command can be used to display information about the configured cflowd collectors.

Example

The following example shows how to display the information about the configured cflowd collectors.

```
Device# show sdwan app-fwd cflowd collector
flow-monitors flow-export-statistics sdwan_flow_exporter_0
export-client
name "options drop-cause-table"
group Option
protocol-stats bytes-added 17220
protocol-stats bytes-sent 17220
protocol-stats bytes-dropped 0
```

```
protocol-stats records-added 492
protocol-stats records-sent 492
protocol-stats records-dropped 0
export-client
name sdwan_flow_monitor
group "Flow Monitor"
protocol-stats bytes-added 0
protocol-stats bytes-sent 0
protocol-stats bytes-dropped 0
protocol-stats records-added 0
protocol-stats records-sent 0
protocol-stats records-dropped 0
export-client
name "options application-attributes"
group Option
protocol-stats bytes-added 377196
protocol-stats bytes-sent 377196
protocol-stats bytes-dropped 0
protocol-stats records-added 1462
protocol-stats records-sent 1462
protocol-stats records-dropped 0
export-client
name "options application-name"
group Option
protocol-stats bytes-added 123670
protocol-stats bytes-sent 123670
protocol-stats bytes-dropped 0
protocol-stats records-added 1490
protocol-stats records-sent 1490
protocol-stats records-dropped 0
```

Table 101: Related Commands

Commands	Description
show sdwan app-fwd cflowd flow-count	Displays cflowd flow count.
show sdwan app-fwd cflowd flows	Displays cflowd flows.
show sdwan app-fwd cflowd statistics	Displays cflowd statistics information.
show sdwan app-fwd cflowd template	Displays cflowd template information.

show sdwan app-fwd cflowd flows

To display cflowd flow information on Cisco IOS XE Catalyst SD-WAN devices, use the **show sdwan app-fwd cflowd flows** command in privileged EXEC mode.

show sdwan app-fwd cflowd flows [**format table** | **vpn** *vpn-id* [**format table**]]

Syntax Description

format table	(Optional) Displays the flows in table format.
vpn *vpn-id*	(Optional) Displays the flows in a specific VPN. The vpn-id range is from 1 to 65530.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Use **show sdwan app-fwd cflowd** command to monitor traffic flowing through Cisco IOS XE Catalyst SD-WAN devices in the overlay network and to export flow information to a collector, where it can be processed by an IPFIX analyzer. Flow-visibility policy must be enabled to see output in this command. This command can be used to display cflowd flow information.

Examples

The following example shows how to display cflowd flow information:

```
Device# show sdwan app-fwd cflowd flows
Generating output, this might take time, please wait ...
app-fwd cflowd flows vpn 32 src-ip 10.3.13.2 dest-ip 10.3.13.10 src-port 41708 dest-port
22 dscp 48 ip-proto 6
 tcp-cntrl-bits       24
 icmp-opcode          0
 total-pkts           45
 total-bytes          2736
 start-time           "Mon Nov 30 17:01:08 2020"
 egress-intf-name     GigabitEthernet0/0/1
 ingress-intf-name    internal0/0/rp:0
 application          unknown
 family               network-service
 drop-cause           "No Drop"
 drop-octets          0
 drop-packets         0
 sla-not-met          0
 color-not-met        0
 queue-id             2
 tos                  255
 dscp-output          63
 sampler-id           3
 fec-d-pkts           0
 fec-r-pkts           0
 pkt-dup-d-pkts-orig  0
 pkt-dup-d-pkts-dup   0
 pkt-dup-r-pkts       0
 pkt-cxp-d-pkts       0
 traffic-category     0
 ssl-read-bytes       0
 ssl-written-bytes    0
 ssl-en-read-bytes    0
 ssl-en-written-bytes 0
 ssl-de-read-bytes    0
 ssl-de-written-bytes 0
 ssl-service-type     0
 ssl-traffic-type     0
 ssl-policy-action    0
```

Table 102: Related Commands

Command	Description
show sdwan app-fwd cflowd collector	Displays cflowd collector information.
show sdwan app-fwd cflowd flow-count	Displays cflowd flow count.
show sdwan app-fwd cflowd statistics	Displays cflowd statistics information.
show sdwan app-fwd cflowd template	Displays cflowd template information.

show sdwan app-fwd cflowd flow-count

To display the number of current cflowd traffic flows on Cisco IOS XE Catalyst SD-WAN devices, use the **show sdwan app-fwd cflowd flow-count** command in privileged EXEC mode.

show sdwan app-fwd cflowd flow-count

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Cflowd monitors traffic flowing through Cisco IOS XE Catalyst SD-WAN devices in the overlay network and exports flow information to a collector, where it can be processed by an IPFIX analyzer. Flow-visibility policy must be enabled to see output from this command. This command can be used to display the number of current cflowd traffic flows.

Examples

The following example shows how to display the number of current cflowd traffic flows.

```
Device# show sdwan app-fwd cflowd flow-count
VPN  COUNT
------------
*    0
```

Table 103: Related Commands

Command	Description
show sdwan app-fwd cflowd collector	Displays cflowd collector information.
show sdwan app-fwd cflowd flows	Displays cflowd flows.

Command	Description
show sdwan app-fwd cflowd statistics	Displays cflowd statistics information.
show sdwan app-fwd cflowd template	Displays cflowd template information.

show sdwan app-fwd cflowd statistics

To display cflowd packet statistics on Cisco IOS XE Catalyst SD-WAN devices, use the **show sdwan app-fwd cflowd statistics** command in privileged EXEC mode.

show sdwan app-fwd cflowd statistics [**ftm** | **dta**]

Syntax Description

ftm	(Optional) Displays cflowd Forwarding Table Manager (FTM) statistics information. From Cisco IOS XE Catalyst SD-WAN Release 17.18.1a FTM is no longer supported. Use DTA instead.
dta	(Optional) Displays cflowd Data Tracking Agent (DTA) statistics information.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command is qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Use **show sdwan app-fwd cflowd** command to monitor traffic flowing through Cisco IOS XE Catalyst SD-WAN devices in the overlay network and to export flow information to a collector, where it can be processed by an IPFIX analyzer. Flow-visibility policy must be enabled to see output from this command. This command can be used to display cflowd packet statistics.

Examples

The following example shows how to display cflowd packet statistics.

```
Device# show sdwan app-fwd cflowd statistics
      data_packets             :      30996
      template_packets         :      36
      total-packets            :      9
      flow-refresh             :      0
      flow-ageout              :      0
      flow-end-detected        :      0
      flow-end-forced          :      0
      flow-rate-limit-drop     :      0
```

Table 104: Related Commands

Command	Description
show sdwan app-fwd cflowd collector	Displays cflowd collector information.
show sdwan app-fwd cflowd flow-count	Displays cflowd flow count.
show sdwan app-fwd cflowd flows	Displays cflowd flows.
show sdwan app-fwd cflowd template	Displays cflowd template information.

show sdwan app-fwd cflowd template

To display the cflowd template information that the Cisco IOS XE Catalyst SD-WAN device transmits periodically to the cflowd collector, use the **show sdwan app-fwd cflowd flows** command in privileged EXEC mode.

show sdwan app-fwd cflowd template

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command is qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Use **show sdwan app-fwd cflowd** to monitor traffic flowing through Cisco IOS XE Catalyst SD-WAN devices in the overlay network and to export flow information to a collector, where it can be processed by an IPFIX analyzer. A cflowd template defines the location of cflowd collectors, how often sets of sampled flows are sent to the collectors, and how often the template is sent to the collectors.

This command can be used to display the cflowd template information that the Cisco IOS XE Catalyst SD-WAN device transmits periodically to the cflowd collector.

Examples

The following example shows how to display the cflowd template information that the Cisco IOS XE Catalyst SD-WAN device transmits periodically to the cflowd collector.

```
Device# show sdwan app-fwd cflowd template
app cflowd template name ""
app cflowd template flow-active-timeout 600
app cflowd template flow-inactive-timeout 60
app cflowd template template-refresh 0
```

Table 105: Related Commands

Command	Description
show sdwan app-fwd cflowd collector	Displays cflowd collector information.
show sdwan app-fwd cflowd flow-count	Displays cflowd flow count.
show sdwan app-fwd cflowd flows	Displays cflowd flows.
show sdwan app-fwd cflowd statistics	Displays cflowd statistics information.

show sdwan app-fwd dpi flows

show sdwan app-fwd dpi flows—Display flow information for the application-aware applications running on the Cisco IOS XE Catalyst SD-WAN device.

show sdwan app-fwd dpi flows [**vpn** *vpn-id*] [**detail**]

Syntax Description

None	List all the flows which go through the Cisco IOS XE Catalyst SD-WAN device
detail	Detailed Information Display detailed information about DPI traffic flows, including total packet and octet counts, and which tunnel (TLOC) the flow was received and transmitted on. **Note** This command displays all the flow information except for Border Gateway Protocols, Internet Control Message Protocol for IPv4, Internet Control Message Protocol for IPv6, Open Shortest Path First, Multicast Transfer Protocol, and Protocol-Independent Multicast in a policy as they are not supported. These application bypass DPI and matching DPI on the applications do not affect a policy.
vpn *vpn-id*	Specific VPN List all application flows running in the subnets in the specific VPN.

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command introduced.

Examples

show sdwan app-fwd dpi flows

```
Device# show sdwan app-fwd dpi flows

app-fwd cflowd flows vpn 7 src-ip 10.7.20.8 dest-ip 10.7.50.10 src-port 0 dest-port 2048
dscp 0 ip-proto 1
 tcp-cntrl-bits           24
 icmp-opcode              2048
 total-pkts               23392
 total-bytes              2339200
 start-time               "Mon Dec 26 09:48:28 2022"
 egress-intf-name         Null
 ingress-intf-name        GigabitEthernet0/0/0
 application              ping
 family                   network-service
 drop-cause               "No Drop"
 drop-octets              0
 drop-packets             0
 sla-not-met              0
 color-not-met            0
 queue-id                 2
 tos                      0
 dscp-output              0
 sampler-id               0
 fec-d-pkts               0
 fec-r-pkts               0
 pkt-dup-d-pkts-orig      0
 pkt-dup-d-pkts-dup       0
 pkt-dup-r-pkts           0
 pkt-cxp-d-pkts           0
 traffic-category         0
 service-area             0
 ssl-read-bytes           0
 ssl-written-bytes        0
 ssl-en-read-bytes        0
 ssl-en-written-bytes     0
 ssl-de-read-bytes        0
 ssl-de-written-bytes     0
 ssl-service-type         0
 ssl-traffic-type         0
 ssl-policy-action        0
 appqoe-action            0
 appqoe-sn-ip             0.0.0.0
 appqoe-pass-reason       0
 appqoe-dre-input-bytes   0
 appqoe-dre-input-packets 0
 appqoe-flags             0

Device# show sdwan app-fwd dpi flows table
Generating output, this might take time, please wait ...


                                                                                                        PKT
   PKT    PKT   PKT                                                    SSL              SSL
                                                                APPQOE  APPQOE
                                                                      TCP

                                  SLA   COLOR                                      FEC    FEC   DUP
D  DUP D  DUP   CXP                     SSL    SSL       EN      SSL EN   DE      SSL DE
SSL      SSL      SSL                     APPQOE  DRE      DRE
                             SRC     DEST          IP      CNTRL  ICMP     TOTAL  TOTAL
```

```
       DROP      DROP     DROP      NOT  NOT    QUEUE       DSCP    SAMPLER  D      R      PKTS
   PKTS    R      D      TRAFFIC   SERVICE  READ   WRITTEN  READ   WRITTEN  READ   WRITTEN
SERVICE  TRAFFIC  POLICY  APPQOE  APPQOE   PASS    INPUT   INPUT    APPQOE
VPN  SRC IP      DEST IP     PORT   PORT   DSCP  PROTO  BITS   OPCODE  PKTS   BYTES    START
 TIME               EGRESS INTF NAME      INGRESS INTF NAME     APPLICATION  FAMILY
     CAUSE    OCTETS  PACKETS  MET  MET    ID     TOS  OUTPUT  ID       PKTS  PKTS  ORIG
 DUP    PKTS  PKTS  CATEGORY  AREA     BYTES  BYTES    BYTES  BYTES    BYTES  BYTES    TYPE
     TYPE     ACTION  ACTION  SN IP    REASON  BYTES   PACKETS  FLAGS
-------------------------------------------------------------------------------------------
7    10.7.20.8   10.7.50.10  0      2048   0     1      24     2048    27886  2788600  Mon
 Dec 26 09:48:28 2022  Null                  GigabitEthernet0/0/0  ping
network-service  No Drop  0       0        0    0      2      0    0       0        0
0     0      0      0     0     0         0        0      0        0      0        0
0        0        0        0       0       0.0.0.0  0       0       0        0
7    10.7.50.10  10.7.20.8   11983  22     48    6      24     0       5625   225072   Mon
 Dec 26 09:48:28 2022  GigabitEthernet0/0/0  internal0/0/rp:0      ssh          terminal
       No Drop  0       0        0    0      2      0    0       0        0      0      0
   0      0     0     0         0        0      0        0      0        0      0        0
         0        0       0       0.0.0.0  0       0       0        0
7    10.7.20.8   10.7.50.10  47897  22     48    6      24     0       10403  416264   Mon
 Dec 26 09:48:28 2022  internal0/0/rp:0      GigabitEthernet0/0/0  ssh          terminal
       No Drop  0       0        0    0      2      0    0       0        0      0      0
   0      0     0     0         0        0      0        0      0        0      0        0
         0        0       0       0.0.0.0  0       0       0        0
7    10.7.50.10  10.7.20.8   22     47897  48    6      24     0       19441  1477468  Mon
 Dec 26 09:48:28 2022  GigabitEthernet0/0/0  internal0/0/rp:0      ssh          terminal
       No Drop  0       0        0    0      2      0    0       0        0      0      0
   0      0     0     0         0        0      0        0      0        0      0        0
         0        0       0       0.0.0.0  0       0       0        0
7    10.7.20.8   10.7.50.10  22     11983  48    6      24     0       10532  800432   Mon
 Dec 26 09:48:28 2022  internal0/0/rp:0      GigabitEthernet0/0/0  ssh          terminal
       No Drop  0       0        0    0      2      0    0       0        0      0      0
   0      0     0     0         0        0      0        0      0        0      0        0
         0        0       0       0.0.0.0  0       0       0        0
                                  SOURCE  DEST
```

```
Device# show sdwan app-fwd dpi flows
app-fwd cflowd flows vpn 7 src-ip 10.7.50.10 dest-ip 10.7.20.8 src-port 11983 dest-port 22
 dscp 48 ip-proto 6
 tcp-cntrl-bits           24
 icmp-opcode              0
 total-pkts               3192
 total-bytes              127716
 start-time               "Mon Dec 26 09:48:28 2022"
 egress-intf-name         GigabitEthernet0/0/0
 ingress-intf-name        internal0/0/rp:0
 application              ssh
 family                   terminal
 drop-cause               "No Drop"
 drop-octets              0
 drop-packets             0
 sla-not-met              0
 color-not-met            0
 queue-id                 2
 tos                      0
 dscp-output              0
 sampler-id               0
 fec-d-pkts               0
 fec-r-pkts               0
 pkt-dup-d-pkts-orig      0
 pkt-dup-d-pkts-dup       0
 pkt-dup-r-pkts           0
```

```
pkt-cxp-d-pkts           0
traffic-category         0
service-area             0
ssl-read-bytes           0
ssl-written-bytes        0
ssl-en-read-bytes        0
ssl-en-written-bytes     0
ssl-de-read-bytes        0
ssl-de-written-bytes     0

ssl-service-type         0
ssl-traffic-type         0
ssl-policy-action        0
appqoe-action            0
appqoe-sn-ip             0.0.0.0
appqoe-pass-reason       0
appqoe-dre-input-bytes   0
appqoe-dre-input-packets 0
appqoe-flags             0
```

show sdwan app-fwd dpi summary

To display the DPI summary on Cisco IOS XE Catalyst SD-WAN devices, use the **show sdwan app-fwd dpi summary** command in privileged EXEC mode.

show sdwan app-fwd dpi summary

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command is qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines Deep Packet Inspection (DPI) offers control over how data packets from specific applications or application families are forwarded across the network, allowing you to assign the traffic to be carried by specific tunnels. App-visibility policy must be enabled to see output from this command.

Use **show sdwan app-fwd dpi summary** command to display the DPI summary on Cisco IOS XE Catalyst SD-WAN devices.

Examples

The following example shows how to display the DPI summary on Cisco IOS XE Catalyst SD-WAN devices.

```
Device# show sdwan app-fwd dpi summary
                                                          ACTIVE  INACTIVE
                                                          FLOWS   FLOWS
                    CACHE  CURRENT  HIGH      FLOWS FLOWS TIMED   TIMED
```

```
NAME                SIZE   ENTRIES  WATERMARK ADDED AGED  OUT     OUT
-------------------------------------------------------------------------------
sdwan_flow_monitor  80000  0        0         0     0      0       0
```

Table 106: Related Commands

Command	Description
show sdwan app-fwd dpi flows	Displays DPI flows.

show sdwan app-route sla-class

To display application-aware routing SLA classes on Cisco IOS XE Catalyst SD-WAN devices, use the **show sdwan app-route sla-class** command in privileged EXEC mode.

show sdwan app-route sla-class
show sdwan app-route sla-class
jitter *jitter-configured-value* | **latency** *latency-configured-value* | **loss** *loss-percentage* | **name** *sla-class-name*

Syntax Description

None	Displays information for all index, name, packet jitter, packet latency, and packet loss values.
jitter *jitter-configured-value*	(Optional) Displays information for all index, name, packet jitter, packet latency, and packet loss values for the specified jitter value in milliseconds. <0 - 4294967295>
latency *latency-configured-value*	(Optional) Displays information for all index, name, packet jitter, packet latency, and packet loss values for the specified latency value in milliseconds. <0 - 4294967295>
loss *loss-percentage*	(Optional) Displays information for all index, name, packet jitter, packet latency, and packet loss values for the specified loss value in percentage. <0 - 100>
name *sla-class-name*	(Optional) Displays information for all index, name, packet jitter, packet latency, and packet loss values for the specified SLA class name.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

The action taken in application-aware routing is applied based on an SLA (a service-level agreement). An SLA class is defined by the maximum jitter, maximum latency, maximum packet loss, or a combination of these values, for the data plane tunnels of the device.

Use this command to display information for application-aware routing SLA classes configured on Cisco IOS XE Catalyst SD-WAN devices.

Example

The following example shows how to display index, name, packet loss, packet latency, and packet jitter information for all application-aware routing SLA classes configured on Cisco IOS XE Catalyst SD-WAN devices.

```
Device# show sdwan app-route sla-class
INDEX NAME LOSS LATENCY JITTER
-----------------------------------------------------
0 __all_tunnels__ 0 0 0
1 test_sla_class 100 50 0
2 test_sla_class2 10 5 50
```

The following example shows how to display index, name, packet loss, packet latency, and packet jitter information for all application-aware routing SLA classes with latency value of 50 configured on Cisco IOS XE Catalyst SD-WAN devices.

```
Device# show sdwan app-route sla-class latency 50
INDEX NAME LOSS LATENCY JITTER
-----------------------------------------------------
1 test_sla_class 100 50 0
```

The following example shows how to display index and packet jitter information for all application-aware routing SLA classes configured on Cisco IOS XE Catalyst SD-WAN devices.

```
Device# show sdwan app-route sla-class jitter
INDEX JITTER
-----------------
0 0
1 0
2 50
```

show sdwan app-route stats

To display statistics about data plane traffic jitter, loss, and latency and other interface characteristics for all operational data plane tunnels on Cisco IOS XE Catalyst SD-WAN devices, use the **show sdwan app-route stats** command in privileged EXEC mode.

show sdwan app-route stats
{ [**local-color** *color*] | [**remote-color** *color*] | [**remote-system-ip** *ip-address*] }

Syntax Description

local-color *color*	(Optional) Displays statistics about data plane traffic jitter, loss, and latency and other interface characteristics for the specified local color.
remote-color *color*	(Optional) Displays statistics about data plane traffic jitter, loss, and latency and other interface characteristics for the specified remote color.

remote-system-ip *ip-address*	(Optional) Displays statistics about data plane traffic jitter, loss, and latency and other interface characteristics for the specified remote system IP.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

The Bidirectional Forwarding Detection (BFD) protocol runs over all data plane tunnels between Cisco IOS XE SD-WAN devices, monitoring the liveness, and network and path characteristics of the tunnels. Application-aware routing uses the information gathered by BFD to determine the transmission performance of the tunnels. Performance is reported in terms of packet latency and packet loss on the tunnel.

BFD sends Hello packets periodically to test the liveness of a data plane tunnel and to check for faults on the tunnel. These Hello packets provide a measurement of packet loss and packet latency on the tunnel. The Cisco IOS XE SD-WAN device records the packet loss and latency statistics over a sliding window of time. BFD keeps track of the six most recent sliding windows of statistics, placing each set of statistics in a separate bucket.

If you configure an application-aware routing policy for the device, it is these statistics that the router uses to determine whether a data plane tunnel's performance matches the requirements of the policy's SLA.

This command can be used to display statistics about data plane traffic jitter, loss, and latency and other interface characteristics for all operational data plane tunnels on Cisco IOS XE SD-WAN devices.

Note The **show sdwan app-route stats** output includes statistics for each data plane tunnel, showing total packets, average loss, average latency, jitter, and transmitted/received data packets.

When SLA is not met and there is no traffic for one Application Performance Class (APC), the statistics from all APCs are averaged internally to calculate measurements for that APC. The output of the `show sdwan app-route stats` command displays these averaged statistics for the APC that is not met.

Example

The following example shows how to display statistics about data plane traffic jitter, loss, and latency and other interface characteristics for all operational data plane tunnels on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan app-route status
app-route statistics 100.64.0.30 100.64.0.2 ipsec 12426 12366
remote-system-ip 10.1.0.1
local-color mpls
remote-color mpls
mean-loss 0
mean-latency 2
mean-jitter 0
sla-class-index 0
IPV6 TX IPV6 RX
```

```
TOTAL AVERAGE AVERAGE TX DATA RX DATA DATA DATA
INDEX PACKETS LOSS LATENCY JITTER PKTS PKTS PKTS PKTS
------------------------------------------------------------------------------
0 6 0 2 0 0 0 0 0
1 6 0 2 1 0 0 0 0
2 5 0 2 0 0 0 0 0
3 6 0 2 0 0 0 0 0
4 5 0 2 0 0 0 0 0
5 6 0 2 0 0 0 0 0
app-route statistics 100.64.2.2 100.64.2.26 ipsec 12366 12366
remote-system-ip 10.1.0.1
local-color biz-internet
remote-color biz-internet
mean-loss 0
mean-latency 11
mean-jitter 9
sla-class-index 0
IPV6 TX IPV6 RX
TOTAL AVERAGE AVERAGE TX DATA RX DATA DATA DATA
INDEX PACKETS LOSS LATENCY JITTER PKTS PKTS PKTS PKTS
------------------------------------------------------------------------------
0 6 0 10 7 10 10 0 0
1 5 0 9 3 0 0 0 0
2 6 0 12 12 11 11 0 0
3 5 0 10 3 0 0 0 0
4 6 0 9 9 10 10 0 0
5 6 0 12 16 0 0 0 0
app-route statistics 100.64.0.30 100.64.0.6 ipsec 12426 12366
remote-system-ip 10.1.0.2
local-color mpls
remote-color mpls
mean-loss 0
mean-latency 2
mean-jitter 0
sla-class-index 0
IPV6 TX IPV6 RX
TOTAL AVERAGE AVERAGE TX DATA RX DATA DATA DATA
INDEX PACKETS LOSS LATENCY JITTER PKTS PKTS PKTS PKTS
------------------------------------------------------------------------------
0 5 0 1 0 0 0 0 0
1 6 0 1 0 0 0 0 0
2 5 0 2 0 0 0 0 0
3 6 0 1 0 0 0 0 0
4 6 0 2 0 0 0 0 0
5 5 0 2 0 0 0 0 0
app-route statistics 100.64.2.2 100.64.2.30 ipsec 12366 12366
remote-system-ip 10.1.0.2
local-color biz-internet
remote-color biz-internet
mean-loss 0
mean-latency 13
mean-jitter 7
sla-class-index 0
IPV6 TX IPV6 RX
TOTAL AVERAGE AVERAGE TX DATA RX DATA DATA DATA
INDEX PACKETS LOSS LATENCY JITTER PKTS PKTS PKTS PKTS
------------------------------------------------------------------------------
0 6 0 16 8 10 12 0 0
1 5 0 12 6 0 0 0 0
2 6 0 10 11 11 12 0 0
3 6 0 14 9 0 0 0 0
4 5 0 14 4 11 11 0 0
5 6 0 14 6 0 0 0 0
```

The following example shows how to display statistics about data plane traffic jitter, loss, and latency and other interface characteristics for the specified local color mpls on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan app-route stats local-color mpls
app-route statistics 100.64.0.30 100.64.0.2 ipsec 12426 12366
remote-system-ip 10.1.0.1
local-color mpls
remote-color mpls
mean-loss 0
mean-latency 2
mean-jitter 0
sla-class-index 0
IPV6 TX IPV6 RX
TOTAL AVERAGE AVERAGE TX DATA RX DATA DATA DATA
INDEX PACKETS LOSS LATENCY JITTER PKTS PKTS PKTS PKTS
------------------------------------------------------------------------------
0 6 0 2 0 0 0 0 0
1 6 0 2 1 0 0 0 0
2 5 0 2 0 0 0 0 0
3 6 0 2 0 0 0 0 0
4 5 0 2 0 0 0 0 0
5 6 0 2 0 0 0 0 0
app-route statistics 100.64.0.30 100.64.0.6 ipsec 12426 12366
remote-system-ip 10.1.0.2
local-color mpls
remote-color mpls
mean-loss 0
mean-latency 2
mean-jitter 0
sla-class-index 0
IPV6 TX IPV6 RX
TOTAL AVERAGE AVERAGE TX DATA RX DATA DATA DATA
INDEX PACKETS LOSS LATENCY JITTER PKTS PKTS PKTS PKTS
------------------------------------------------------------------------------
0 5 0 1 0 0 0 0 0
1 6 0 1 0 0 0 0 0
2 5 0 2 0 0 0 0 0
3 6 0 1 0 0 0 0 0
4 6 0 2 0 0 0 0 0
5 5 0 2 0 0 0 0 0
```

The following example shows how to display statistics about data plane traffic jitter, loss, and latency and other interface characteristics for the specified remote system IP 10.1.0.1 on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan app-route stats remote-system-ip 10.1.0.1

app-route statistics 100.64.0.30 100.64.0.2 ipsec 12426 12366
remote-system-ip 10.1.0.1
local-color mpls
remote-color mpls
mean-loss 0
mean-latency 2
mean-jitter 0
sla-class-index 0
IPV6 TX IPV6 RX
TOTAL AVERAGE AVERAGE TX DATA RX DATA DATA DATA
INDEX PACKETS LOSS LATENCY JITTER PKTS PKTS PKTS PKTS
------------------------------------------------------------------------------
0 6 0 2 0 0 0 0 0
1 6 0 2 1 0 0 0 0
```

```
2 5 0 2 0 0 0 0 0
3 6 0 2 0 0 0 0 0
4 5 0 2 0 0 0 0 0
5 6 0 2 0 0 0 0 0
app-route statistics 100.64.2.2 100.64.2.26 ipsec 12366 12366
remote-system-ip 10.1.0.1
local-color biz-internet
remote-color biz-internet
mean-loss 0
mean-latency 11
mean-jitter 9
sla-class-index 0
IPV6 TX IPV6 RX
TOTAL AVERAGE AVERAGE TX DATA RX DATA DATA DATA
INDEX PACKETS LOSS LATENCY JITTER PKTS PKTS PKTS PKTS
------------------------------------------------------------------------------
0 6 0 10 7 10 10 0 0
1 5 0 9 3 0 0 0 0
2 6 0 12 12 11 11 0 0
3 5 0 10 3 0 0 0 0
4 6 0 9 9 10 10 0 0
5 6 0 12 16 0 0 0 0
```

Related Commands

Command	Description
show sdwan app-route sla-class	Displays application-aware routing SLA classes.

show sdwan bfd history

To display Cisco Catalyst SD-WAN BFD history on Cisco IOS XE Catalyst SD-WAN devices, use the **show sdwan bfd history** command in privileged EXEC mode.

show sdwan bfd history

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE SD-WAN Release 17.2.1v	This command is supported for Cisco Catalyst SD-WAN.
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	The command output shows BFD automatic suspension information.

Usage Guidelines

BFD provides rapid failure detection times between forwarding engines, while maintaining low overhead. If a BFD session is down, it implies that no traffic can flow between those TLOCs. If you identify any traffic disruption between a pair of TLOCs or notice that the session flap count has increased, use the **show sdwan bfd history** command to check the history of your BFD sessions.

Use this command to display Cisco Catalyst SD-WAN BFD history on Cisco IOS XE Catalyst SD-WAN devices.

Example

The following example shows how to display Cisco Catalyst SD-WAN BFD history on Cisco IOS XE Catalyst SD-WAN devices.



Note Beginning with Cisco IOS XE Catalyst SD-WAN Release 17.10.1a, a suspended flag, `Sus`, is added for identifying BFD sessions that are suspended for preventing flapping of BFD sessions.

Related Commands

Command	Description
request platform software sdwan auto-suspend reset	Brings all BFD sessions out of suspension.
show sdwan bfd sessions	Displays Cisco Catalyst SD-WAN BFD sessions.
show sdwan bfd summary	Displays a Cisco Catalyst SD-WAN BFD summary.
show sdwan bfd tloc-summary-list	Displays a Cisco Catalyst SD-WAN BFD TLOC summary list.

show sdwan bfd sessions

To display information about the Cisco SD-WAN BFD sessions on Cisco IOS XE Catalyst SD-WAN devices, use the **show sdwan bfd sessions** command in privileged EXEC mode.

show sdwan bfd sessions [**table** | **alt** | **region-access** | **region-core** | **suspend** { **all** | **local-color** *local-color-value* }]

Syntax Description

table	(Optional) Display output in table format.
alt	(Optional) Display additional information for BFD sessions, such as BFD local discriminator (LD) and if a BFD session is flagged as suspended.
region-access	(Optional) Multi-Region Fabric access region.
region-core	(Optional) Multi-Region Fabric core region.
suspend	(Optional) Display BFD sessions in suspension.
all	(Optional) Display all BFD sessions in suspension.
local-color *local-color-value*	(Optional) Display BFD sessions with a local color.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	This command is supported for Cisco Catalyst SD-WAN.
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	This command was modified. Added the **suspend** and **alt** keywords. The command output shows BFD automatic suspension information.

Usage Guidelines

BFD provides rapid failure detection times between forwarding engines, while maintaining low overhead. If a BFD session is down, it implies that no traffic can flow between those TLOCs. If you identify any traffic disruption between a pair of TLOCs or notice that the session flap count has increased, use the **show sdwan bfd sessions** command to check the status of your Cisco SD-WAN BFD sessions.

Use this command to display information about the Cisco SD-WAN BFD sessions running on Cisco IOS XE Catalyst SD-WAN devices.

Examples

The following sample output from the **show sdwan bfd sessions** command displays information about the Cisco SD-WAN BFD sessions running on Cisco IOS XE Catalyst SD-WAN devices.

```
Device# show sdwan bfd sessions
                                SOURCE TLOC    REMOTE TLOC               DST PUBLIC   DST PUBLIC        DETECT      TX
SYSTEM IP  SITE ID STATE  COLOR          COLOR         SOURCE IP   IP           PORT       ENCAP  MULTIPLIER  INTERVAL(msec) UPTIME      TRANSITIONS
-----------------------------------------------------------------------------------------------------------------------------------------------------

10.1.0.1   100     up     biz-internet   biz-internet  10.64.2.2  10.64.2.26  12366       ipsec    7           1000           0:00:03:14  0
10.1.0.2   100     up     biz-internet   biz-internet  10.64.2.2  10.64.2.30  12366       ipsec    7           1000           0:00:03:13  0
10.4.0.1   400     up     biz-internet   biz-internet  10.64.2.2  10.64.2.6   18464       ipsec    7           1000           0:00:03:14  0
```

The following sample output from the **show sdwan bfd sessions suspend** command displays the total suspend count and the resuspend count.

```
Device# show sdwan bfd sessions suspend

                     SOURCE TLOC   REMOTE TLOC               DST PUBLIC       DST PUBLIC         RE-SUSPEND  SUSPEND       TOTAL     SUSPEND
SYSTEM IP        STATE    COLOR         COLOR         SOURCE IP      IP               PORT        ENCAP  COUNT       TIME LEFT     COUNT     DURATION
-----------------------------------------------------------------------------------------------------------------------------------------------
172.16.255.14    up       lte           lte           10.1.15.15     10.1.14.14       12426       ipsec  0           0:00:19:52    18        0:00:00:07
```

The following sample output from the **show sdwan bfd sessions alt** command indicates if a BFD session has been suspended:

```
Device# show sdwan bfd sessions alt

*Sus = Suspend
*NA  = Flag Not Set
                                    SOURCE TLOC    REMOTE TLOC               DST PUBLIC      DST PUBLIC
SYSTEM IP        SITE ID   STATE    COLOR          COLOR         SOURCE IP   IP              PORT        ENCAP  BFD-LD    FLAGS   UPTIME
-----------------------------------------------------------------------------------------------------------------------------------------------
172.16.255.14    400       up        3g             lte          10.0.20.15  10.1.14.14      12426       ipsec  20004     NA      0:19:30:40
172.16.255.14    400       up        lte            lte          10.1.15.15  10.1.14.14      12426       ipsec  20003     Sus     0:00:02:46
172.16.255.16    600       up        3g             lte          10.0.20.15  10.0.106.1      12366       ipsec  20002     NA      0:19:30:40
172.16.255.16    600       up        lte            lte          10.1.15.15  10.0.106.1      12366       ipsec  20001     NA      0:19:20:14
```

The following sample output from the **show sdwan bfd sessions table** command displays the traffic with ports in the control range:

```
Device# show sdwan bfd sessions table
                        SRC    DST                 SITE                                  DETECT      TX
SRC IP      DST IP      PROTO  PORT   PORT   SYSTEM IP      ID    LOCAL COLOR   COLOR        STATE  MULTIPLIER  INTERVAL  UPTIME      TRANSITIONS
-----------------------------------------------------------------------------------------------------------------------------------------------
```

```
10.1.15.15  10.0.5.11   ipsec  12366  12367  172.16.255.11  100   lte           lte           up     7          1000      0:01:37:43  3
10.1.19.15  10.0.5.11   ipsec  12406  12367  172.16.255.11  100   biz-internet  lte           up     7          1000      0:00:00:51  0
10.1.15.15  10.1.14.14  ipsec  12366  12366  172.16.255.14  400   lte           lte           up     7          1000      0:01:37:43  3
10.1.19.15  10.1.14.14  ipsec  12406  12366  172.16.255.14  400   biz-internet  lte           up     7          1000      0:00:00:51  0
10.1.15.15  10.1.16.16  ipsec  12366  12386  172.16.255.16  600   lte           biz-internet  up     7          1000      0:00:31:41  0
10.1.19.15  10.1.16.16  ipsec  12406  12386  172.16.255.16  600   biz-internet  biz-internet  down   7          1000      NA          0
10.1.15.15  10.0.5.21   ipsec  12366  12377  172.16.255.21  100   lte           lte           up     7          1000      0:01:37:43  3
10.1.19.15  10.0.5.21   ipsec  12406  12377  172.16.255.21  100   biz-internet  lte           up     7          1000      0:00:00:51  0
```

Related Commands

Command	Description
request platform software sdwan auto-suspend reset	Brings all BFD sessions out of suspension.
show sdwan bfd history	Displays Cisco SD-WAN BFD history.
show sdwan bfd summary	Displays a Cisco SD-WAN BFD summary.
show sdwan bfd tloc-summary-list	Displays a Cisco SD-WAN BFD TLOC summary list.

show sdwan bfd sessions region-access

To display a list of bidirectional forwarding detection (BFD) sessions in the Hierarchical SD-WAN access region (any region other than the core region), use the **show sdwan bfd sessions region-access** command in privileged EXEC mode.

sdwan sdwan bfd sessions region-access

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Examples

```
Device# show sdwan bfd sessions region-access
                                REGION             SOURCE TLOC    REMOTE TLOC                                    DST PUBLIC                    DST
PUBLIC          DETECT      TX
SYSTEM IP         SITE ID  ID     STATE       COLOR          COLOR          SOURCE IP                            IP                            PORT
        ENCAP  MULTIPLIER  INTERVAL(msec) UPTIME          TRANSITIONS
-------------------------------------------------------------------------------------------------------------------------------------------------
172.21.54.10     2100     2      up          lte            lte            172.16.21.11                         172.16.1.1                    12366
       ipsec  7           1000           12:04:30:17     6
172.21.55.10     2200     2      up          lte            lte            172.16.21.11                         172.16.2.1                    12366
       ipsec  7           1000           12:04:29:47     8
172.21.14.10     22200    2      up          lte            lte            172.16.21.11                         172.16.22.11                  12366
       ipsec  7           1000           12:04:35:03     7
172.21.54.10     2100     2      up          lte            3g             172.16.21.11                         172.17.1.1                    12366
       ipsec  7           1000           12:04:30:01     7
172.21.55.10     2200     2      up          lte            3g             172.16.21.11                         172.17.2.1                    12366
       ipsec  7           1000           12:04:30:05     7
172.21.14.10     22200    2      up          lte            3g             172.16.21.11                         172.17.22.11                  12366
       ipsec  7           1000           12:04:29:27     9
172.21.54.10     2100     2      up          3g             lte            172.17.21.11                         172.16.1.1                    12366
       ipsec  7           1000           12:04:29:27     8
172.21.55.10     2200     2      up          3g             lte            172.17.21.11                         172.16.2.1                    12366
       ipsec  7           1000           12:04:29:26     8
172.21.14.10     22200    2      up          3g             lte            172.17.21.11                         172.16.22.11                  12366
       ipsec  7           1000           12:04:29:26     8
172.21.54.10     2100     2      up          3g             3g             172.17.21.11                         172.17.1.1                    12366
       ipsec  7           1000           12:04:29:27     8
172.21.55.10     2200     2      up          3g             3g             172.17.21.11                         172.17.2.1                    12366
       ipsec  7           1000           12:04:29:26     9
172.21.14.10     22200    2      up          3g             3g             172.17.21.11                         172.17.22.11                  12366
       ipsec  7           1000           12:04:29:26     0
```

show sdwan bfd sessions region-core

To display a list of bidirectional forwarding detection (BFD) sessions in the Hierarchical SD-WAN core region, use the **show sdwan bfd sessions region-core** command in privileged EXEC mode.

sdwan sdwan bfd sessions region-core

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Examples

```
Device# show sdwan bfd sessions region-core
                          REGION              SOURCE TLOC     REMOTE TLOC                                    DST PUBLIC                    DST
 PUBLIC          DETECT      TX
SYSTEM IP        SITE ID   ID     STATE       COLOR           COLOR          SOURCE IP                       IP                            PORT
        ENCAP   MULTIPLIER  INTERVAL(msec) UPTIME          TRANSITIONS
-------------------------------------------------------------------------------------------------------------------------------------------
172.20.11.10     11100     0      up          green           green          172.18.21.11                    172.23.11.11                  12366
       ipsec  7           1000           12:04:29:40     7
172.20.12.10     11100     0      up          green           green          172.18.21.11                    172.23.12.11                  12366
       ipsec  7           1000           12:04:29:40     6
172.21.14.10     22200     0      up          green           green          172.18.21.11                    172.18.22.11                  12366
       ipsec  7           1000           12:04:29:38     10
172.19.15.10     33100     0      up          green           green          172.18.21.11                    172.19.31.11                  12366
       ipsec  7           1000           12:04:29:37     5
```

show sdwan bfd summary

To display Cisco SD-WAN BFD summary information on Cisco IOS XE SD-WAN devices, use the **show sdwan bfd summary** command in privileged EXEC mode.

show sdwan bfd summary [{ **bfd-sessions-total** | **bfd-sessions-up** | **bfd-sessions-max** | **bfd-sessions-flap** | **poll-interval** }]

Syntax Description

bfd-sessions-total	(Optional) Displays only the current number of BFD sessions running.
bfd-sessions-up	(Optional) Displays only the current number of BFD sessions that are in the Up state.
bfd-sessions-max	(Optional) Displays only the total number of BFD sessions that have been created since the device booted up.
bfd-sessions-flap	(Optional) Displays only the number of BFD sessions that have transitioned from the Up state.
poll-interval	(Optional) Displays only the poll interval of all tunnels in milliseconds.

Command Default

None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE SD-WAN Release 17.2.1v	This command is supported for Cisco Catalyst SD-WAN.
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	The command output shows BFD automatic suspension information.

Usage Guidelines BFD provides rapid failure detection times between forwarding engines, while maintaining low overhead. If a BFD session is down, it implies that no traffic can flow between those TLOCs. If you identify any traffic disruption between a pair of TLOCs or notice that the session flap count has increased, use the **show sdwan bfd summary** command to check the status of your BFD sessions.

Use this command to display Cisco SD-WAN BFD summary information on Cisco IOS XE SD-WAN devices.

Example

The following example shows how to display a Cisco SD-WAN BFD session summary on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan bfd summary
sessions-total 2
sessions-up 2
sessions-max 2
sessions-flap 8
poll-interval 600000
```

The following example shows how to display only the current number of Cisco SD-WAN BFD sessions that are in the up state on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan bfd summary bfd-sessions-up
bfd summary bfd-sessions-up 2
```

The following example shows how to display a Cisco SD-WAN BFD session summary, including which Cisco SD-WAN BFD sessions have been suspended.

```
Device# show sdwan bfd summary
sessions-total           4
sessions-up              4
sessions-max             4
sessions-flap            4
poll-interval            60000
sessions-up-suspended    1
sessions-down-suspended  0
```

Related Commands

Command	Description
request platform software sdwan auto-suspend reset	Brings all BFD sessions out of suspension.
show sdwan bfd history	Displays Cisco SD-WAN BFD history.
show sdwan bfd sessions	Displays Cisco SD-WAN BFD sessions.
show sdwan bfd tloc-summary-list	Displays a Cisco SD-WAN BFD TLOC summary list.

show sdwan bfd tloc-summary-list

To display Cisco SD-WAN BFD session summary information per TLOC on Cisco IOS XE SD-WAN devices, use the **show sdwan bfd tloc-summary-list** command in privileged EXEC mode.

show sdwan bfd tloc-summary-list [*interface-name*]

Syntax Description

interface-name	(Optional) Displays BFD session summary information on the specified interface.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE SD-WAN Release 17.2.1v	This command is supported for Cisco Catalyst SD-WAN.
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	The command output shows BFD automatic suspension information.

Usage Guidelines

BFD provides rapid failure detection times between forwarding engines, while maintaining low overhead. If a BFD session is down, it implies that no traffic can flow between those TLOCs. If you identify any traffic disruption between a pair of TLOCs or notice that the session flap count has increased, use the **showsdwanbfdtloc-summary-list** command to check the status of your BFD sessions per TLOC.

You can use this command to display Cisco SD-WAN BFD session summary information per TLOC on Cisco IOS XE SD-WAN devices.

Example

The following example shows how to display Cisco SD-WAN BFD session summary information for all TLOCs on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan bfd tloc-summary-list

SESSIONS SESSIONS SESSIONS
IF NAME ENCAP TOTAL UP FLAP
-----------------------------------------------------------
GigabitEthernet0/0/0 ipsec 2 2 8
GigabitEthernet0/0/1 ipsec 2 2 10
```

The following example shows how to display Cisco SD-WAN BFD session summary information on the specified interface GigabitEthernet0/0/0 on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan bfd tloc-summary-list GigabitEthernet0/0/0

SESSIONS SESSIONS SESSIONS
IF NAME ENCAP TOTAL UP FLAP
-----------------------------------------------------------
GigabitEthernet0/0/0 ipsec 2 2 8
```

The following example shows how to display Cisco SD-WAN BFD session summary information that includes information for BFD sessions that are up, sessions that are suspended, and sessions that are down and suspended.

```
Device# show sdwan bfd tloc-summary-list
                                                                  SESSIONS    SESSIONS
                          SESSIONS  SESSIONS  SESSIONS  UP          DOWN
IF NAME             ENCAP TOTAL     UP        FLAP      SUSPENDED   SUSPENDED

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

GigabitEthernet1    ipsec     2       2         4          1          0
GigabitEthernet4    ipsec     2       2         0          0          0
```

Related Commands

Command	Description
request platform software sdwan auto-suspend reset	Brings all BFD sessions out of suspension.
show sdwan bfd history	Displays Cisco SD-WAN BFD history.
show sdwan bfd sessions	Displays Cisco SD-WAN BFD sessions.
show sdwan bfd summary	Displays Cisco SD-WAN BFD summary.

show sdwan certificate

To display information about the sdwan certificates on Cisco IOS XE Catalyst SD-WAN devices, use the **show sdwan certificate** command in privileged EXEC mode.

show sdwan certificate { **installed** | **reverse-proxy** | **root-ca-cert** | **serial** | **signing-request** | **validity** }

Syntax Description

installed	Displays sdwan certificate installed.
root-ca-cert	Displays sdwan certificate root-ca-cert.
reverse-proxy	Displays the signed certificate installed on a Cisco IOS XEE SD-WAN device for authentication with a reverse proxy device.
serial	Displays sdwan certificate serial.
signing-request	Displays sdwan certificate signing-request.
validity	Displays sdwan certificate validity.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Support introduced for the keyword **reverse-proxy**.

Usage Guidelines

In the SD-WAN solution, we focus on building secure data plane connections, which involves onboarding physical or virtual WAN edge devices and establishing secure control connections across all the SD-WAN components in the network environment.

Secure onboarding of the SD-WAN edge physical or virtual device requires the device to be identified, trusted and allowed in the same overlay network.

Identity of the WAN edge device is uniquely identified by the chassis ID and certificate serial number. Depending on the WAN edge router, certificates are provided in different ways:

- Hardware-based Cisco IOS XE Catalyst SD-WAN device certificate is stored in the on-board SUDI chip installed during manufacturing.
- Virtual platform (Cisco CSR 1000v) which do not have root certificates preinstalled on the device. For these devices, a One-Time Token (OTK) is provided by Cisco SD-WAN Manager to authenticate the device with the SD-WAN controllers.

Trust of the WAN edge devices is done using the root chain certificates that are pre-loaded in manufacturing, loaded manually, distributed automatically by Cisco SD-WAN Manager, or installed during the Cisco Plug-and-Play automated deployment provisioning process.

The Cisco Catalyst SD-WAN solution uses a model, where the WAN edge devices that are allowed to join the SD-WAN overlay network need to be known by all the SD-WAN controllers beforehand. This is done by adding the WAN edge devices in the Plug-and-Play connect portal (PnP).

Use **show sdwan certificate** command to display information about the Cisco SD-WAN certificates on Cisco IOS XE Catalyst SD-WAN devices to be used for Plug-and-Play, bootstrap or manual onboarding.

Example

The following example shows how to display the decoded certificate signing request installed on Cisco IOS XE Catalyst SD-WAN devices.

```
Device# show sdwan certificate installed
Board-id certificate
--------------------
Certificate:
Data:
Version: 3 (0x2)
Serial Number: 69965125 (0x43bd3a8)
Signature Algorithm: sha256WithRSAEncryption
Issuer: O=Cisco, CN=ACT2 SUDI CA
Validity
Not Before: Aug 5 14:19:01 2019 GMT
Not After : May 14 20:25:41 2029 GMT
Subject: serialNumber=PID:ISR4331/K9 SN:SAMPLESN123, O=Cisco, OU=ACT-2 Lite SUDI,
CN=ISR4331/K9
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public-Key: (2048 bit)
Modulus:
00:cb:cd:16:b1:1f:76:f2:ca:21:4d:9f:32:e5:ef:
79:f4:00:c3:98:15:18:17:20:2d:f3:c4:86:2a:3a:
16:64:4a:e8:f9:93:57:31:87:ae:b5:6d:0a:d7:c2:
93:6c:f6:b2:db:41:7e:0a:16:7f:13:dc:e6:30:35:
f8:1e:e3:e7:20:00:10:2e:71:08:f6:c1:91:8a:1b:
80:d3:a8:cf:df:97:f1:7c:3f:df:2e:1f:d7:27:dd:
02:da:af:98:06:7e:83:3a:83:7a:1e:1f:9f:99:ea:
5f:1a:7c:02:0c:21:10:60:76:db:fe:d9:92:5b:cd:
1b:7e:a6:78:9c:04:10:9f:71:cb:52:90:59:09:9f:
```

```
1b:93:48:28:ce:38:e6:d7:db:dd:88:7a:c9:1c:f3:
eb:0b:ab:8c:a2:2a:01:be:27:3e:b1:1c:fe:bc:90:
fb:71:c4:58:c3:41:b0:22:2b:49:93:96:53:58:bf:
16:64:4a:e8:f9:93:57:31:87:ae:b5:6d:0a:d7:c2:
1c:fa:17:d9:4f:53:98:d9:63:ab:c9:54:b0:ef:b9:
8e:1f:d8:70:fd:ef:14:d2:35:96:5b:02:3d:16:23:
03:86:ed:be:6b:34:01:0a:25:66:b5:98:73:b0:3f:
5f:1a:7c:02:0c:21:10:60:76:db:fe:d9:92:5b:cd:
03:86
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Key Usage: critical
Digital Signature, Non Repudiation, Key Encipherment
X509v3 Basic Constraints: critical
CA:FALSE
X509v3 Subject Alternative Name:
othername:<unsupported>
Signature Algorithm: sha256WithRSAEncryption
7b:6c:21:4f:1b:25:73:46:d8:27:79:4c:37:70:a9:b3:57:d7:
24:55:73:11:cc:cb:17:3b:d3:e4:5d:a9:88:8f:92:c8:d8:a4:
41:09:b9:52:a0:45:e4:8f:d2:03:d9:26:8d:cc:59:69:14:e9:
77:e7:ab:30:bf:a5:e8:41:bd:3a:16:9e:91:4f:4b:d3:12:9f:
6d:0a:11:c8:46:d8:81:1b:63:6f:89:22:b6:87:8e:6b:6b:0d:
73:d1:8c:60:77:4e:a3:69:8d:a3:1f:c8:7a:15:ad:d2:68:39:
37:13:25:34:74:4c:b6:05:17:7a:09:6e:83:ed:43:dd:6b:0a:
21:9a:0b:4c:13:63:01:1f:92:ad:19:26:14:fe:0e:2d:86:32:
a6:b0:3f:8f:8e:c4:f9:67:df:03:e9:cb:a3:db:02:bb:44:8c:
24:55:73:11:cc:cb:17:3b:d3:e4:5d:a9:88:8f:92:c8:d8:a4:
ff:39:8a:9b:b4:eb:4d:e8:37:b1:6e:e8:f2:27:ea:85:c1:b3:
6d:0a:11:c8:46:d8:81:1b:63:6f:89:22:b6:87:8e:6b:6b:0d:
27:02:46:b1:cd:91:b9:cc:6e:85:97:a4:67:c7:d1:e0:55:0e:
65:70:ed:79:17:86:9a:70:70:70:8b:a9:e3:81:0b:e5:42:b8:
21:9a:0b:4c
Installed device certificates
-----------------------------
```

The following example shows how to display the root certificate installed on Cisco IOS XE Catalyst SD-WAN devices.

```
Device# show sdwan certificate root-ca-cert
Certificate:
Data:
Version: 3 (0x2)
Serial Number:
b9:a5:54:a0:5b:ac:6b:88
Signature Algorithm: sha256WithRSAEncryption
Issuer: C = US, ST = Texas, L = Dallas, O = Test_Name, OU = Test_Name
Validity
Not Before: Aug 31 21:15:48 2020 GMT
Not After : Dec 9 21:15:48 2020 GMT
Subject: C = US, ST = Texas, L = Dallas, O = Test_Name, OU = Test_Name
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public-Key: (2048 bit)
Modulus:
ac:4e:7b:e5:e9:b4:cd:84:95:4d:38:63:c4:a8:52:
e4:35:6e:ec:8b:55:54:a2:91:51:c1:41:e5:48:5f:
20:f6:48:08:2f:d7:bc:1e:c7:a4:dd:27:27:36:25:
5c:26:01:c9:1e:8f:fe:18:0d:94:23:46:a0:24:2f:
ac:24:d9:4b:81:99:ba:ed:71:45:1a:ea:17:03:e7:
ac:4e:7b:e5:e9:b4:cd:84:95:4d:38:63:c4:a8:52:
18:3c:6f:ec:1e:fe:37:31:4d:a7:58:7c:07:ac:06:
88:3e:47:ea:7e:27:d6:21:31:10:dc:5d:30:db:14:
20:f6:48:08:2f:d7:bc:1e:c7:a4:dd:27:27:36:25:
```

```
ac:4e:7b:e5:e9:b4:cd:84:95:4d:38:63:c4:a8:52:
97:80:ef:37:e2:96:4f:93:9e:2f:bb:22:7a:cc:bb:
6f:2c:f8:52:b2:f2:07:3c:a9:cc:c6:b2:72:00:c8:
e3:a4:ad:36:fe:70:16:8a:28:48:5c:90:00:d6:8b:
20:f6:48:08:2f:d7:bc:1e:c7:a4:dd:27:27:36:25:
72:1a:56:0b:f2:84:8f:09:fd:0b:42:7e:19:fd:43:
ac:4e:7b:e5:e9:b4:cd:84:95:4d:38:63:c4:a8:52:
70:a0:dc:2e:43:8f:f1:f3:b7:d6:a7:89:d4:41:5d:
f6:73
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Subject Key Identifier:
54:45:B0:9E:ED:59:3E:D5:9F:03:38:F2:3A:44:C0:E3:6A:CB:86:4C
X509v3 Authority Key Identifier:
keyid:54:45:B0:9E:ED:59:3E:D5:9F:03:38:F2:3A:44:C0:E3:6A:CB:86:4C
X509v3 Basic Constraints:
CA:TRUE
Signature Algorithm: sha256WithRSAEncryption
28:85:ea:02:06:1d:65:1f:ab:47:ac:c9:e3:6c:45:4a:0b:dd:
a3:6c:ae:f5:7e:4d:0c:ba:15:7e:e9:b1:d0:81:61:fd:93:72:
8a:0d:21:dc:53:c0:18:4d:8a:dc:3f:bf:76:91:1d:15:4f:72:
28:85:ea:02:06:1d:65:1f:ab:47:ac:c9:e3:6c:45:4a:0b:dd:
ea:f4:e8:de:83:c3:5d:b0:a6:e3:8b:e8:52:db:03:da:26:f3:
9f:67:fe:57:a6:03:b0:5d:47:a6:2b:2b:27:90:57:c6:ca:da:
23:0f:7a:00:78:5d:92:e1:91:c5:f7:ce:f7:e7:09:6f:5b:f9:
28:85:ea:02:06:1d:65:1f:ab:47:ac:c9:e3:6c:45:4a:0b:dd:
9f:67:fe:57:a6:03:b0:5d:47:a6:2b:2b:27:90:57:c6:ca:da:
fd:df:ed:26:f4:1b:39:ab:cf:af:f9:b1:bd:64:7e:72:e4:42:
20:1b:52:96:69:63:46:af:32:7a:45:fe:96:e8:55:14:e1:79:
74:a8:2a:ca:5c:34:ea:cc:2c:35:3a:84:da:df:dd:85:3d:db:
9f:67:fe:57:a6:03:b0:5d:47:a6:2b:2b:27:90:57:c6:ca:da:
28:85:ea:02:06:1d:65:1f:ab:47:ac:c9:e3:6c:45:4a:0b:dd:
98:b3:4f:bc
```

The following example shows how to display the chassis number, board ID serial number, and serial number on Cisco IOS XE Catalyst SD-WAN devices.

```
Device# show sdwan certificate serial
Chassis number: ISR4331/K9-SAMPLESN123 Board ID serial number: 053BE1B7 Subject S/N:
SAMPLESN123
```

The following example shows how to display how long a certificate is valid for on Cisco IOS XE Catalyst SD-WAN devices.

```
Device# show sdwan certificate validity
The certificate is valid from Aug 5 14:19:01 2019 GMT (Current date is Mon Nov 30 22:01:08
 GMT 2020) & valid until May 14 20:25:41 2029 GMT
```

The following is a sample output from the execution of the **show sdwan certificate reverse-proxy** command on a Cisco IOS XE SD-WAN device.

```
Device#show sdwan certificate reverse-proxy

Reverse proxy certificate

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



Certificate:

    Data:

        Version: 1 (0x0)
```

```
        Serial Number: 1 (0x1)

        Signature Algorithm: sha256WithRSAEncryption

        Issuer: C = US, CN = 6c63e80a-8175-47de-a455-53a127ee70bd, O = Viptela

        Validity

            Not Before: Jun  2 19:31:08 2021 GMT

            Not After : May 27 19:31:08 2051 GMT

        Subject: C = US, ST = California, CN = C8K-9AE4A5A8-4EB0-E6C1-1761-6E54E4985F78, O
= ViptelaClient
        Subject Public Key Info:

            Public Key Algorithm: rsaEncryption

                RSA Public-Key: (2048 bit)

                Modulus:

                    00:e2:45:49:53:3a:56:d4:b8:70:59:90:01:fb:b1:

                    44:e3:73:17:97:a3:e9:b7:55:44:d4:2d:dd:13:4a:

                    a8:ef:78:14:9d:bd:b5:69:de:c9:31:29:bd:8e:57:

                    09:f2:02:f8:3d:1d:1e:cb:a3:2e:94:c7:2e:61:ea:

                    e9:94:3b:28:8d:f7:06:12:56:f3:24:56:8c:4a:e7:

                    01:b1:2b:1b:cd:85:4f:8d:34:78:78:a1:26:17:2b:

                    a5:1b:2a:b6:dd:50:51:f8:2b:13:93:cd:a6:fd:f8:

                    71:95:c4:db:fc:a7:83:05:23:68:61:15:05:cc:aa:

                    60:af:09:ef:3e:ce:70:4d:dd:50:84:3c:9a:57:ce:

                    cb:15:84:3e:cd:b2:b6:30:ab:86:68:17:94:fa:9c:

                    1a:ab:28:96:68:8c:ef:c8:f7:00:8a:7a:01:ca:58:

                    84:b0:87:af:9a:f6:13:0f:aa:42:db:8b:cc:6e:ba:

                    c8:c1:48:d2:f4:d8:08:b1:b5:15:ca:36:80:98:47:

                    32:3a:df:54:35:fe:75:32:23:9f:b5:ed:65:41:99:

                    50:b9:0f:7a:a2:10:59:12:d8:3e:45:78:cb:dc:2a:

                    95:f2:72:02:1a:a6:75:06:87:52:4d:01:17:f2:62:

                    8c:40:ad:29:e4:75:17:04:65:a9:b9:6a:dd:30:95:

                    34:9b

                Exponent: 65537 (0x10001)

    Signature Algorithm: sha256WithRSAEncryption

         99:40:af:23:bb:cf:7d:59:e9:a5:83:78:37:02:76:83:79:02:
```

```
b3:5c:56:e8:c3:aa:fc:78:ef:07:23:f8:14:19:9c:a4:5d:88:

07:4d:6e:b8:0d:b5:af:fa:5c:f9:55:d0:60:94:d9:24:99:5e:
33:06:83:03:c3:73:c1:38:48:45:ba:6a:35:e6:e1:51:0e:92:

c3:a2:4a:a2:e1:2b:da:cd:0c:c3:17:ef:35:52:e1:6a:23:20:

af:99:95:a2:cb:99:a7:94:03:f3:78:99:bc:76:a3:0f:de:04:

7d:35:e1:dc:4d:47:79:f4:c8:4c:19:df:80:4c:4f:15:ab:f1:

61:a2:78:7a:2b:6e:98:f6:7b:8f:d6:55:44:16:79:e3:cd:51:

0e:27:fc:e6:4c:ff:bb:8f:2d:b0:ee:ed:98:63:e9:c9:cf:5f:

d7:b1:dd:7b:19:32:22:94:77:d5:bc:51:85:65:f3:e0:93:c7:

3c:79:fc:34:c7:9f:40:dc:b1:fc:6c:e5:3d:af:2d:77:b7:c3:

88:b3:89:7c:a6:1f:56:35:3b:35:66:0c:c8:05:b5:28:0b:98:

19:c7:b0:8e:dc:b7:3f:9d:c1:bb:69:f0:7d:20:95:b5:d1:f0:

06:35:b7:c4:64:ba:c4:95:31:4a:97:03:0f:04:54:6d:cb:50:

2f:31:02:59


Device#
```

show sdwan certificate staged

To display the certificate currently in the staging process on a device in the SD-WAN device solution, use the **show sdwan certificate staged** command in EXEC mode.

show sdwan certificate staged

Command Default

This command has no default behavior.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.18.1a	This command was introduced.

Usage Guidelines

For information about staging certificates, see How Cisco SD-WAN Manager installs a new certificate on an edge device in the *Cisco Catalyst SD-WAN Getting Started Guide*.

This command applies to WAN edge devices in the SD-WAN device solution. For devices in the SD-Routing device solution, see show sd-routing certificate staged, on page 1274.

While a device has a certificate in staging, which can take a minute or more, this command displays the certificate details. After the device completes the staging and testing of the certificate, the certificate is cleared and the command output does not show a certificate.

Example

This example shows the output of the command when a certificate is in staging. The output is abbreviated.

```
Device#show sdwan certificate staged
Staged certificate
------------------------------
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number:
            04:4d:…
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, ST = CA, L = San Jose, OU = Acme, O = Cisco Systems Inc, CN = ca
        Validity
            Not Before: Sep 20 16:52:32 2024 GMT
            Not After : Sep 18 16:52:32 2034 GMT
        Subject: C = US, ST = CA, L = San Jose, OU = Acme, O = Cisco Systems Inc, CN = ce5
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:aa:11:bb:22:cc:33:dd:44:ee:55:ff:66:77:88:
                    …
```

Related Commands

Command	Description
show sd-routing certificate staged	Display the certificate currently in the staging process on a device in the SD-Routing device solution.

show sdwan cloudexpress applications

To display the best path that Cloud onRamp for SaaS has selected for each configured SaaS application, on Cisco IOS XE Catalyst SD-WAN devices, use the **show sdwan cloudexpress applications** command in privileged EXEC mode.

show sdwan cloudexpress applications

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 17.2	This command was introduced.
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	The command output may include the Webex application, which is supported from this release.

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	The command output may include custom applications, which are supported from this release. The output header includes information about the application ID, application type, and the sub-application ID.

Usage Guidelines

The command output includes sections for each configured SaaS application.

Examples

The following is a sample output from the **show sdwan cloudexpress applications** command, as it appears in Cisco IOS XE Catalyst SD-WAN Release 17.8.1a, showing a standard SaaS application (amazon_aws).

```
Device# show sdwan cloudexpress applications
cloudexpress applications vpn 1 app 3 type app-group subapp 0
 application amazon_aws
 exit-type   local
 interface   GigabitEthernet5
 latency     2
 loss        1
```

Table 107: Command Output Header Field Descriptions, Beginning with Cisco IOS XE Catalyst SD-WAN Release 17.8.1a

Output	Description
vpn	Each VPN for which Cloud onRamp for SaaS is enabled appears in the output.
app	Application ID corresponding to the application.
type	Possible values are: app-group, custom-app-group, region
subapp	Sub-application ID corresponding to the application. An application can have one or more sub-application ID's.

The following is a sample output from the **show sdwan cloudexpress applications** command, as it appears in Cisco IOS XE Catalyst SD-WAN Release 17.8.1a, showing the Webex app, which is of type region.

```
Device# show sdwan cloudexpress applications
cloudexpress applications vpn 1 app 15 type region subapp 8
 application webex-us-west-1
 exit-type   local
 interface   GigabitEthernet5
 latency     139
 loss        0
```

The following is a sample output from the **show sdwan cloudexpress applications** command, as it appears in Cisco IOS XE Catalyst SD-WAN Release 17.8.1a, showing a user-defined SaaS application list called example-apps.

```
Device# show sdwan cloudexpress applications
cloudexpress applications vpn 2 app 26 type custom-app-group subapp 0
 application example-apps
```

```
 exit-type   local
 interface   GigabitEthernet5
 latency     66
 loss        0
```

The following is a sample output from the **show sdwan cloudexpress applications** command, as it appears beginning with Cisco IOS XE Catalyst SD-WAN Release 17.7.1a.

```
Device# show sdwan cloudexpress applications
cloudexpress applications vpn 1 app-group 3
 application amazon_aws
 exit-type   local
 interface   GigabitEthernet5.101
 latency     3
 loss        0
cloudexpress applications vpn 1 region 8
 application webex-us-west-1
 exit-type   none
 latency     0
 loss        0
```

The following is a sample output from the **show sdwan cloudexpress applications** command, as it appears before Cisco IOS XE Catalyst SD-WAN Release 17.7.1a.

```
Device# show sdwan cloudexpress applications
cloudexpress applications vpn 1 office365
exit-type local
interface GigabitEthernet1
latency   1
loss      40
cloudexpress applications vpn 1 amazon_aws
exit-type         gateway
gateway-system-ip 10.0.0.1
latency           1
loss              0
local-color       lte
remote-color      lte
cloudexpress applications vpn 1 dropbox
exit-type         gateway
gateway-system-ip 10.0.0.1
latency           19
loss              0
local-color       lte
remote-color      lte
```

show sdwan cloudexpress gateway-exits

show sdwan cloudexpress gateway-exits—Display loss and latency on each gateway exit for applications configured with Cloud OnRamp for SaaS (formerly called CloudExpress service).

show sdwan cloudexpress gateway-exits

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	This command was introduced.
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	The command output may include the Webex application, which is supported from this release.
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	The command output may include custom applications, which are supported from this release. The output header includes information about the application ID, application type, and the sub-application ID.

Usage Guidelines

The command output includes sections for each configured SaaS application.

Examples

The following is a sample output from the **show sdwan cloudexpress gateway-exits** command, as it appears in Cisco IOS XE Catalyst SD-WAN Release 17.8.1a, showing a standard SaaS application (amazon_aws).

```
Device# show sdwan cloudexpress gateway-exits
cloudexpress gateway-exits vpn 1 app 3 type app-group subapp 0 192.168.1.15
 application  amazon_aws
 latency      1
 loss         1
 local-color  lte
 remote-color lte
```

Table 108: Command Output Header Field Descriptions, Beginning with Cisco IOS XE Catalyst SD-WAN Release 17.8.1a

Output	Description
vpn	Each VPN for which Cloud onRamp for SaaS is enabled appears in the output.
app	Application ID corresponding to the application.
type	Possible values are: app-group, custom-app-group, region
subapp	Sub-application ID corresponding to the application. An application can have one or more sub-application ID's.

The following is a sample output from the **show sdwan cloudexpress gateway-exits** command, as it appears in Cisco IOS XE Catalyst SD-WAN Release 17.8.1a, showing the Webex app, which is of type region.

```
Device# show sdwan cloudexpress gateway-exits
cloudexpress gateway-exits vpn 1 app 15 type region subapp 1 192.168.1.15
 application  webex-us-west-1
 latency      139
 loss         0
 local-color  lte
 remote-color lte
```

The following is a sample output from the **show sdwan cloudexpress gateway-exits** command, as it appears in Cisco IOS XE Catalyst SD-WAN Release 17.8.1a, showing a user-defined SaaS application list called example-apps.

```
Device# show sdwan cloudexpress gateway-exits
cloudexpress gateway-exits vpn 1 app 26 type custom-app-group subapp 0 192.168.1.15
 application  example-apps
 latency      66
 loss         0
 local-color  lte
 remote-color lte
```

The following example shows the command output, as it appears in releases earlier than Cisco IOS XE Catalyst SD-WAN Release 17.7.1a.

```
Device# show sdwan cloudexpress gateway-exits
cloudexpress gateway-exits vpn 1 office365 172.16.255.15
latency 2
loss 0
local-color lte
remote-color lte
cloudexpress gateway-exits vpn 1 office365 172.16.255.16
latency 2
loss 0
local-color lte
remote-color lte
cloudexpress gateway-exits vpn 1 amazon_aws 172.16.255.15
latency 1
loss 0
local-color lte
remote-color lte
cloudexpress gateway-exits vpn 1 amazon_aws 172.16.255.16
latency 1
loss 0
local-color lte
remote-color lte
```

show sdwan cloudexpress load-balance applications

To view the interface, exit type, and statistics for the best path that Cloud onRamp for SaaS has selected for each configured SaaS application, on Cisco IOS XE Catalyst SD-WAN devices, use the **show sdwan cloudexpress load-balance applications** command in privileged EXEC mode.

show sdwan cloudexpress load-balance applications

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	This command was introduced.
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	The command output may include the Webex application, which is supported from this release.

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	The command output may include custom applications, which are supported from this release. The output header includes information about the application ID, application type, and the sub-application ID.

Examples

The following is a sample output from the **show sdwan cloudexpress load-balance applications** command, as it appears in Cisco IOS XE Catalyst SD-WAN Release 17.8.1a.

```
Device# show sdwan cloudexpress load-balance applications
cloudexpress load-balance applications-lb vpn 1 app 3 type app-group subapp 0 GigabitEthernet5
application amazon_aws
exit-type local
latency 2
loss 4
cloudexpress load-balance applications-lb vpn 1 app 3 type app-group subapp 0 GigabitEthernet6
application amazon_aws
exit-type local
latency 1
loss 2
```

Table 109: Command Output Header Field Descriptions, Beginning with Cisco IOS XE Catalyst SD-WAN Release 17.8.1a

Output	Description
vpn	Each VPN for which Cloud onRamp for SaaS is enabled appears in the output.
app	Application ID corresponding to the application.
type	Possible values are: app-group, custom-app-group, region
subapp	Sub-application ID corresponding to the application. An application can have one or more sub-application ID's.

The following is a sample output from the **show sdwan cloudexpress load-balance applications** command, as it appears before Cisco IOS XE Catalyst SD-WAN Release 17.7.1a.

```
Device# show sdwan cloudexpress load-balance applications
cloudexpress load-balance applications-lb vpn 10 office365 GigabitEthernet1
exit-type local
latency 1
loss 5
cloudexpress load-balance applications-lb vpn 10 office365 GigabitEthernet2
exit-type local
latency 1
loss 7
```

Table 110: Command Output Header Field Descriptions, Beginning with Cisco IOS XE Catalyst SD-WAN Release 17.8.1a

Output	Description
vpn	Each VPN for which Cloud onRamp for SaaS is enabled appears in the output.

```
Device# show sdwan cloudexpress load-balance applications
cloudexpress load-balance applications-lb vpn 10 office365 GigabitEthernet1
exit-type local
latency 1
loss 5
cloudexpress load-balance applications-lb vpn 10 office365 GigabitEthernet2
exit-type local
latency 1
loss 7
```

show sdwan cloudexpress local-exits

show sdwan cloudexpress local-exits—Display application loss and latency on each Direct Internet Access (DIA) interface enabled for Cloud OnRamp for SaaS (formerly called CloudExpress service).

show sdwan cloudexpress local-exits

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	This command was introduced.
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	The command output may include the Webex application, which is supported from this release.
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	The command output may include custom applications, which are supported from this release. The output header includes information about the application ID, application type, and the sub-application ID.

Usage Guidelines

The command output includes sections for each configured SaaS application.

Examples

The following is a sample output from the **show sdwan cloudexpress local-exits** command, as it appears in Cisco IOS XE Catalyst SD-WAN Release 17.8.1a, showing a standard SaaS application (amazon_aws).

```
Device# show sdwan cloudexpress local-exits
cloudexpress local-exits vpn 1 app 3 type app-group subapp 0 GigabitEthernet5
 application amazon_aws
 latency     1
 loss        2
```

Table 111: Command Output Header Field Descriptions, Beginning with Cisco IOS XE Catalyst SD-WAN Release 17.8.1a

Output	Description
vpn	Each VPN for which Cloud onRamp for SaaS is enabled appears in the output.
app	Application ID corresponding to the application.
type	Possible values are: app-group, custom-app-group, region
subapp	Sub-application ID corresponding to the application. An application can have one or more sub-application ID's.

The following is a sample output from the **show sdwan cloudexpress local-exits** command, as it appears in Cisco IOS XE Catalyst SD-WAN Release 17.8.1a, showing the Webex app, which is of type region.

```
Device# show sdwan cloudexpress local-exits
cloudexpress local-exits vpn 1 app 15 type region subapp 1 GigabitEthernet5
 application webex-us-west-1
 latency     139
 loss        0
```

The following is a sample output from the **show sdwan cloudexpress local-exits** command, as it appears in Cisco IOS XE Catalyst SD-WAN Release 17.8.1a, showing a user-defined SaaS application list called example-apps.

```
Device# show sdwan cloudexpress local-exits
cloudexpress local-exits vpn 1 app 26 type custom-app-group subapp 0 GigabitEthernet5
 application example-apps
 latency     66
 loss        0
```

show sdwan cloudexpress local-exits

The following is a sample output from the **show sdwan cloudexpress local-exits** command, as it appears in releases earlier than Cisco IOS XE Catalyst SD-WAN Release 17.7.1a.

```
Device# show sdwan cloudexpress local-exits

VPN APPLICATION INTERFACE LATENCY LOSS
------------------------------------------------------------------------
1 office365 Tunnel100015 10 0
1 office365 Tunnel100016 3 0
1 amazon_aws Tunnel100015 10 0
1 amazon_aws Tunnel100016 3 0
```

show sdwan control

To display information about the control connections and control plane connections on Cisco IOS XE SD-WAN devices, use the **show sdwan control** command in privileged EXEC mode.

show sdwan control

{ **affinity** { **config** | **status** } | **connection-history** | **connection-info** | **connections** | **local-properties** | **statistics** | **summary** | **valid-vmanage-id** | **valid-vsmarts** }

Syntax Description

affinity config	Displays the configuration information about the control connections to one or more Cisco Catalyst SD-WAN Controllers.
affinity status	Displays the status of the control connections to one or more Cisco Catalyst SD-WAN Controllers.
connection-history	Displays the status of the control connections to one or more Cisco Catalyst SD-WAN Controllers.
connection-info	Displays information about the control plane connections.
connections	Displays information about active control plane connections.
local-properties	Displays the basic configuration parameters and local properties related to the control plane. If you configure an enterprise certificate for a Cisco Catalyst 8000V device using Cisco SD-WAN Manager, the **enterprise-cert** fields in the output do not show any information. For hardware devices, these fields are populated correctly. From Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, in case of an expired certificate, the **certificate-validity** field in the command output shows **Valid - Expired**. In earlier releases, it shows only **Expired**.
statistics	Displays statistics about the packets that a device has transmitted and received in the process of establishing and maintaining secure DTLS connections to devices in the overlay network.
summary	Displays a count of devices that the local device is aware.
valid-vmanage-id	Displays the chassis number of the Cisco SD-WAN Manager instances.
valid-vsmarts	Displays the serial numbers of the valid Cisco Catalyst SD-WAN Controllers in the overlay network.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	Added the Hierarchical SD-WAN region assignment to the the **REG IDs** column when you use the **local-properties** keyword.

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	For Hierarchical SD-WAN architectures, the **REGION IDs** column shows the secondary region also.
Cisco IOS XE Catalyst SD-WAN Release 17.14.1a	Updated the output when using the **local-properties** keyword. In case of an expired certificate, the **certificate-validity** field in the command output shows **Valid - Expired**.

Usage Guidelines

In the Cisco SD-WAN overlay network, all Cisco XE SD-WAN devices and Cisco WAN Edge devices establish control connections to all Cisco Catalyst SD-WAN Controllers, to ensure that the routers are always able to properly route data traffic across the network.

One way to manage network scale is to configure affinity between Cisco Catalyst SD-WAN Controllers and WAN Edge routers. To do this, you place each Cisco Catalyst SD-WAN Controller into a controller group, and then you configure which group or groups a WAN Edge router can establish control connections with.

The controller groups are what establishes the affinity between Cisco Catalyst SD-WAN Controllers and WAN Edge routers.

The Cisco SD-WAN control plane operates in conjunction with redundant components to ensure that the overlay network remains resilient if one of the components fails.

This command can be used to display information about the control connections and control plane connections on Cisco IOS XE SD-WAN devices.

Example

The following example shows how to display the configuration information about the control connections to one or more Cisco Catalyst SD-WAN Controllers on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan control affinity config

EFFECTIVE CONTROLLER LIST FORMAT - G(C),... - Where G is the Controller Group ID
C is the Required vSmart Count
CURRENT CONTROLLER LIST FORMAT - G(c)s,... - Where G is the Controller Group ID
c is the current vSmart count
s Status Y when matches, N when does not match
EFFECTIVE
REQUIRED LAST-RESORT
INDEX INTERFACE VS COUNT EFFECTIVE CONTROLLER LIST CURRENT CONTROLLER LIST EQUILIBRIUM
INTERFACE
----------------------------------------------------------------------------------------------------
0 GigabitEthernet0/0/0 2 0(2) 0(2)Y Yes No
1 GigabitEthernet0/0/1 2 0(2) 0(2)Y Yes No
```

The following example shows how to display information about control plane connection attempts initiated by the local device on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan control connection-history

Legend for Errors
ACSRREJ - Challenge rejected by peer. NOVMCFG - No cfg in vmanage for device.
BDSGVERFL - Board ID Signature Verify Failure. NOZTPEN - No/Bad chassis-number entry in
ZTP.
BIDNTPR - Board ID not Initialized. OPERDOWN - Interface went oper down.
BIDNTVRFD - Peer Board ID Cert not verified. ORPTMO - Server's peer timed out.
BIDSIG - Board ID signing failure. RMGSPR - Remove Global saved peer.
CERTEXPRD - Certificate Expired RXTRDWN - Received Teardown.
```

```
CRTREJSER - Challenge response rejected by peer. RDSIGFBD - Read Signature from Board ID
failed.
CRTVERFL - Fail to verify Peer Certificate. SERNTPRES - Serial Number not present.
CTORGNMMIS - Certificate Org name mismatch. SSLNFAIL - Failure to create new SSL context.
DCONFAIL - DTLS connection failure. STNMODETD - Teardown extra vBond in STUN server mode.
DEVALC - Device memory Alloc failures. SYSIPCHNG - System-IP changed.
DHSTMO - DTLS HandShake Timeout. SYSPRCH - System property changed
DISCVBD - Disconnect vBond after register reply. TMRALC - Timer Object Memory Failure.
DISTLOC - TLOC Disabled. TUNALC - Tunnel Object Memory Failure.
DUPCLHELO - Recd a Dup Client Hello, Reset Gl Peer. TXCHTOBD - Failed to send challenge to
 BoardID.
DUPSER - Duplicate Serial Number. UNMSGBDRG - Unknown Message type or Bad Register msg.
DUPSYSIPDEL- Duplicate System IP. UNAUTHEL - Recd Hello from Unauthenticated peer.
HAFAIL - SSL Handshake failure. VBDEST - vDaemon process terminated.
IP_TOS - Socket Options failure. VECRTREV - vEdge Certification revoked.
LISFD - Listener Socket FD Error. VSCRTREV - vSmart Certificate revoked.
MGRTBLCKD - Migration blocked. Wait for local TMO. VB_TMO - Peer vBond Timed out.
MEMALCFL - Memory Allocation Failure. VM_TMO - Peer vManage Timed out.
NOACTVB - No Active vBond found to connect. VP_TMO - Peer vEdge Timed out.
NOERR - No Error. VS_TMO - Peer vSmart Timed out.
NOSLPRCRT - Unable to get peer's certificate. XTVMTRDN - Teardown extra vManage.
NEWVBNOVMNG- New vBond with no vMng connections. XTVSTRDN - Teardown extra vSmart.
NTPRVMINT - Not preferred interface to vManage. STENTRY - Delete same tloc stale entry.
HWCERTREN - Hardware vEdge Enterprise Cert Renewed HWCERTREV - Hardware vEdge Enterprise
Cert Revoked.
EMBARGOFAIL - Embargo check failed
PEER PEER
PEER PEER PEER SITE DOMAIN PEER PRIVATE PEER PUBLIC LOCAL REMOTE REPEAT
TYPE PROTOCOL SYSTEM IP ID ID PRIVATE IP PORT PUBLIC IP PORT LOCAL COLOR STATE ERROR ERROR
 COUNT DOWNTIME
------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------
vbond dtls 0.0.0.0 0 0 10.6.16.252 12346 10.6.16.252 12346 public-internet tear_down DISCVBD
 NOERR 0
2020-11-16T21:07:53+0000
vmanage dtls 1.1.1.254 1001 0 10.6.16.254 12346 10.6.16.254 12346 public-internet tear_down
 DISTLOC NOERR
 0 2020-11-16T21:07:34+0000
vsmart dtls 1.1.1.251 1001 1 10.6.16.251 12346 10.6.16.251 12346 public-internet tear_down
 DISTLOC NOERR
0 2020-11-16T21:07:34+0000
vsmart dtls 1.1.1.250 1001 1 10.6.16.250 12346 10.6.16.250 12346 public-internet tear_down
 DISTLOC NOERR
0 2020-11-16T21:07:34+0000
vbond dtls 0.0.0.0 0 0 10.6.16.252 12346 10.6.16.252 12346 public-internet tear_down DISCVBD
 NOERR 0
2020-11-16T13:57:52+0000
```

The following example shows how to display information about control plane connections on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan control connection-info

control connections-info "Per-Control Connection Rate: 300 pps"
```

The following example shows how to display information about active control plane connections on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan control connections

PEER PEER CONTROLLER
PEER PEER PEER SITE DOMAIN PEER PRIV PEER PUB GROUP
TYPE PROT SYSTEM IP ID ID PRIVATE IP PORT PUBLIC IP PORT LOCAL COLOR
PROXY STATE UPTIME ID
------------------------------------------------------------------------
```

```
------------------------------------------------------------
vsmart dtls 1.1.1.250 1001 1 10.6.16.250 12346 10.6.16.250 12346
public-internet No up 14:03:03:35 0
vsmart dtls 1.1.1.251 1001 1 10.6.16.251 12346 10.6.16.251 12346
public-internet No up 14:03:03:33 0
vmanage dtls 1.1.1.254 1001 0 10.6.16.254 12346 10.6.16.254 12346
public-internet No up 14:03:03:31 0
```

The following example shows how to display the basic configuration parameters and local properties related to the control plane on Cisco IOS XE SD-WAN devices.

Note As shown in this example, if you configure an enterprise certificate for a Cisco Catalyst 8000V device using Cisco SD-WAN Manager, the enterprise-cert fields in the output do not show any information. For hardware devices, these fields are populated correctly.

```
Device# show sdwan control local-properties

personality vedge
sp-organization-name Test_Name
organization-name Test_Name
root-ca-chain-status Installed
certificate-status Installed
certificate-validity Valid
certificate-not-valid-before Aug 05 14:19:01 2019 GMT
certificate-not-valid-after May 14 20:25:41 2029 GMT
enterprise-cert-status Not-Applicable
enterprise-cert-validity Not Applicable
enterprise-cert-not-valid-before Not Applicable
enterprise-cert-not-valid-after Not Applicable
dns-name 10.6.16.252
site-id 206
domain-id 1
protocol dtls
tls-port 0
system-ip 10.3.206.1
chassis-num/unique-id ISR4331/K9-SAMPLESN123
serial-num 053DA5B7
subject-serial-num SAMPLESN123
enterprise-serial-num No certificate installed
token -NA-
keygen-interval 1:00:00:00
retry-interval 0:00:00:16
no-activity-exp-interval 0:00:00:20
dns-cache-ttl 0:00:02:00
port-hopped TRUE
time-since-last-port-hop 14:20:44:35
embargo-check success
number-vbond-peers 0
number-active-wan-interfaces 1
NAT TYPE: E -- indicates End-point independent mapping
A -- indicates Address-port dependent mapping
N -- indicates Not learned
Note: Requires minimum two vbonds to learn the NAT type
PUBLIC PUBLIC PRIVATE PRIVATE PRIVATE MAX RESTRICT/ LAST SPI TIME NAT VM
INTERFACE IPv4 PORT IPv4 IPv6 PORT VS/VM COLOR STATE CNTRL CONTROL/ LR/LB CONNECTION REMAINING
 TYPE CON
STUN PRF
------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------
GigabitEthernet0/0/0 10.3.6.2 12366 10.3.6.2 :: 12366 2/1 public-internet up 2 no/yes/no
```

```
No/No
14:20:44:17 0:03:15:24 N 5
```

As per the preceding output

- The last connection time indicates the time when the last vBond connection was attempted over a TLOC.
- The SPI time remaining indicates how long the current Security Parameters Index (SPI) will be valid before the corresponding TLOC rekeys and negotiates a new one.

The following example shows how to display statistics about the packets that a device has transmitted and received in the process of establishing and maintaining secure DTLS connections to devices in the overlay network on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan control statistics

Tx Statistics:
--------------
packets 6544303
octets 448205710
error 0
blocked 0
hello 3947942
connects 0
registers 4
register-replies 0
dtls-handshake 8
dtls-handshake-failures 0
dtls-handshake-done 8
challenge 0
challenge-response 8
challenge-ack 0
challenge-errors 0
challenge-response-errors 0
challenge-ack-errors 0
challenge-general-errors 0
vmanage-to-peer 0
register_to_vmanage 2
Rx Statistics:
--------------
packets 5860730
octets 732977621
errors 0
hello 3947931
connects 0
registers 0
register-replies 4
dtls-handshake 0
dtls-handshake-failures 0
dtls-handshake-done 0
challenge 8
challenge-response 0
challenge-ack 8
challenge-failures 0
vmanage-to-peer 2
register_to_vmanage 0
challenge_failed_due_to_bid 0
```

The following example shows how to display a count of devices that the local device is aware of on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan control summary

control summary 0
vbond_counts 0
vmanage_counts 1
vsmart_counts 2
```

The following example shows how to display the chassis number of the Cisco SD-WAN Manager instances on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan control valid-vmanage-id

CHASSIS NUMBER
--------------------------------------
5271ea7c-edb1-420b-be9a-4d25756785bd
```

The following example shows how to display the serial numbers and organization names of the valid Cisco Catalyst SD-WAN Controllers in the overlay network on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan control valid-vsmarts

SERIAL NUMBER ORG
----------------------------
B137996B88AA876A Test_Name
B137996B88AA876D Test_Name
B137996B88AA876E Test_Name
```

show sdwan debugs

To display the list of enabled SD-WAN debugs on Cisco IOS XE SD-WAN devices, use the **show sdwan debugs** command in privileged EXEC mode.

show sdwan debugs
[confd | config-mgr | dbgd | fpm | ftm | netconf | omp | policy-counter | ttm | vdaemon]

Syntax Description

confd	(Optional) Displays the list of enabled SD-WAN confd debugs.
config-mgr	(Optional) Displays the list of enabled D-WAN config-mgr debugs.
dbgd	(Optional) Displays the list of enabled SD-WAN dbgd debugs.
fpm	(Optional) Displays the list of enabled SD-WAN config-mgr debugs.
ftm	(Optional) Displays the list of enabled SD-WAN config-mgr debugs.
netconf	(Optional) Displays the list of enabled SD-WAN config-mgr debugs.
omp	(Optional) Displays the list of enabled SD-WAN config-mgr debugs.

policy-counter	(Optional) Displays the list of enabled SD-WAN config-mgr debugs.
ttm	(Optional) Displays the list of enabled SD-WAN config-mgr debugs.
vdaemon	(Optional) Displays the list of enabled SD-WAN config-mgr debugs.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

The output from debug commands provides diagnostic information that include a variety of internet working events relating to protocol status and network activity in general.

Debug output is placed in the bootflash/tracelogs folder on the local device.

This command can be used to display the list of enabled sdwan debugs on Cisco IOS XE SD-WAN devices.

Example

The following example shows how to display the list of all enabled SD-WAN debugs on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan debugs
debugs ftm nat
debugs config-mgr events low
debugs confd snmp
debugs cloudexpress omp low
debugs cloudexpress ftm high
```

The following example shows how to display the list of enabled SD-WAN debugs with only specified debug keyword on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan debugs confd
debugs confd snmp
```

Related Commands

Command	Description
debug	Debugging functions.
undebug	Disables debugging functions.

show sdwan firmware-packages details

To display the details of a firmware package that has been loaded on a device but has not been activated, use the **show sdwan firmware-packages details** command in privileged EXEC mode.

show sdwan firmware-packages details

Command Modes Privileged EXEC mode

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	This command was introduced.

Usage Guidelines The device can have one of two states:

- A single firmware package is loaded and activated: The command has no output.
- One firmware package is loaded and activated, and another package has been loaded but not activated: The command output shows the version and additional details of the loaded firmware package, designated as not active.

Example

```
Router#show sdwan firmware-packages details
                              MODEM     SUB PACKAGE
VERSION      PACKAGE TYPE     TYPE      VERSION       ACTIVE
-------------------------------------------------------------
17.6.0.0.1    Modem-Firmware  EM7430    02.33.03.00   false

Total Space:387M Used Space:145M Available Space:237M
```

show sdwan firmware-packages list

To display the firmware packages loaded on a device and the status of the packages (activated or not), use the **show sdwan firmware-packages list** command in privileged EXEC mode.

show sdwan firmware-packages list

Command Default None

Command Modes Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	This command was introduced.

Usage Guidelines

The device can have one of two states:

- A single firmware package is loaded and activated: The command output shows:
  - The version of the firmware package, designated as active
  - Total and used storage space on the device
- One firmware package is loaded and activated, and another package has been loaded but not activated: The command output shows:
  - The version of the active firmware package, designated as active
  - The version of the package that has been loaded but not yet activated, designated as not active
  - Total and used storage space on the device

Example

```
Router#show sdwan firmware-packages list
VERSION       ACTIVE
----------------------
0.0.0         true
17.6.0.0.1    false

Total Space:387M Used Space:145M Available Space:237M
```

show sdwan from-vsmart commit-history

To verify the commit history for a centralized data policy on Cisco IOS XE Catalyst SD-WAN devices, use the **show sdwan from-vsmart commit-history** command in privileged EXEC mode.

show sdwan from-vsmart commit-history { **detail** | **last-xml** | **summary** }

Syntax Description

detail	Displays the commit history details based on the configuration received from the Cisco SD-WAN Controller.
last-xml	Displays the last XML received from the Cisco SD-WAN Controller.
summary	Displays the commit history summary based on the configuration received from the Cisco SD-WAN Controller.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.9.2a	This command was introduced.
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	This command was introduced.

Usage Guidelines

Use the **show sdwan from-vsmart commit-history** command to check which peer has pushed data to the Cisco IOS XE Catalyst SD-WAN device, how much time it took to commit the centralized data policy, and the commit status. You can use the information obtained from this command for troubleshooting policy commit failures and to identity the exact reason for the commit failure.



Note Data is not retained upon a reboot of the Cisco IOS XE Catalyst SD-WAN device. Data displays for all policy-related commits until you reboot the Cisco IOS XE Catalyst SD-WAN device.

Example

The following sample output from the **show sdwan from-vsmart commit-history summary** command displays the commit history for the specified centralized data policies:

```
Device# show sdwan from-vsmart commit-history summary
Index  Tenant   Peer-IP           TIMESTAMP            TIME(secs)  TYPE           STATUS
-------------------------------------------------------------------------------------------
0      0        172.16.255.19      2022-09-21 19:00:39  0.395       POLICY         Success
1      0        172.16.255.19      2022-09-21 19:00:39  0.120       TAG-INSTANCES  Success
2      0        172.16.255.19      2022-09-21 19:07:20  0.357       POLICY         Success
```

The following sample output from the **show sdwan from-vsmart commit-history last-xml** command displays the last XML received from the Cisco SD-WAN Controller:

```
Device# show sdwan from-vsmart commit-history last-xml
vSmart Configuration Commit Last XML Details
-----------------------------------------------------
Index: 2
Peer-IP: 172.16.255.19
XML: <data-policy>
  <name>DP_CEDGE</name>
  <vpn-list>
    <name>vpn1</name>
    <sequence>
      <seq-value>11</seq-value>
      <match>
        <source-ip>10.20.24.17/32</source-ip>
        <source-ip>10.20.24.150/32</source-ip>
        <protocol>1</protocol>
      </match>
      <action>
        <action-value>accept</action-value>
        <count>count1-dp1</count>
      </action>
    </sequence>
   <default-action>accept</default-action>
  </vpn-list>
<direction>all</direction></data-policy><lists><vpn-list>
  <name>vpn1</name>
  <vpn>
    <id>1</id>
  </vpn>
</vpn-list>
</lists>
```

The following sample output from the **show sdwan from-vsmart commit-history detail** command displays the commit history details based on the configuration received from the Cisco SD-WAN Controller:

```
Device# show sdwan from-vsmart commit-history detail
vSmart Configuration Commit History Details
---------------------------------------------------
Index: 0
    Tenant Id: 0
    Peer-IP: 172.16.255.19
    TIMESTAMP: 2022-09-21 19:00:39
    TOTAL-TIME: 0.395 secs
    TYPE: POLICY
    CHKSUM: 0x89da0ad7
    STATUS: Success
    Error-code: n/a
    Error: n/a
Index: 1
    Tenant Id: 0
    Peer-IP: 172.16.255.19
    TIMESTAMP: 2022-09-21 19:00:39
    TOTAL-TIME: 0.120 secs
    TYPE: TAG-INSTANCES
    CHKSUM: 0x9a0b0195
    STATUS: Success
    Error-code: n/a
    Error: n/a
Index: 2
    Tenant Id: 0
    Peer-IP: 172.16.255.19
    TIMESTAMP: 2022-09-21 19:07:20
    TOTAL-TIME: 0.357 secs
    TYPE: POLICY
    CHKSUM: 0x23b98c55
    STATUS: Success
    Error-code: n/a
    Error: n/a
```

show sdwan from-vsmart policy

To display a centralized data policy, an application-aware policy, or a cflowd policy that a Cisco SD-WAN Controller has pushed to the devices, use the **show sdwan from-vsmart policy** command in privileged EXEC mode. The Cisco SD-WAN Controller pushes the policy via OMP after it has been configured and activated on the controller.

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	This command was introduced.
Cisco IOS XE Catalyst SD-WAN Release 17.16.1a	This command is no longer supported. Use the **show sdwan policy from-vsmart** command instead.

show sdwan from-vsmart policy [**app-route-policy**] [**cflowd-template** *template-option*] [**data-policy**] [**lists** { **data-prefix-list** | **vpn-list** }] [**policer**] [**sla-class**]

Syntax Description

None	Display all the data policies that the vSmart controller has pushed to the Cisco IOS XE Catalyst SD-WAN device.

app-route-policy	Display only the application-aware routing policies that the Cisco vSmart controller has pushed to the Cisco IOS XE Catalyst SD-WAN device.
cflowd-template [*template-option*]	Display only the cflowd template information that the Cisco vSmart controller has pushed to the Cisco IOS XE Catalyst SD-WAN device. *template-option* can be one of **collector**, **flow-active-timeout**, **flow-inactive-timeout**, and **template-refresh**.
data-policy	Display only the data policies that the Cisco vSmart controller has pushed to the Cisco IOS XE Catalyst SD-WAN device.
lists {**data-prefix-list** | **vpn-list**}	Display only the policy-related lists that the Cisco vSmart controller has pushed to the Cisco IOS XE Catalyst SD-WAN device.
policer	Display only the policers that the Cisco vSmart controller has pushed to the Cisco IOS XE Catalyst SD-WAN device.
sla-class	Display only the SLA classes for application-aware routing that the Cisco vSmart controller has pushed to the Cisco IOS XE Catalyst SD-WAN device.

Examples

The following is a sample output from the **show sdwan from-vsmart policy** command displaying policy downloaded from Cisco SD-WAN Controller:

```
Device# show sdwan from-vsmart policy
from-vsmart sla-class SLA1
 latency 100
from-vsmart data-policy DATA_POLICY
 direction from-service
 vpn-list vpn_1
  sequence 11
   match
    destination-port         5060
    protocol                 17
    source-tag-instance      DP_V4_TAG1
    destination-tag-instance DP_V4_TAG3
   action accept
    count src_dst_legacy_v4
  sequence 21
   match
    source-tag-instance DP_V4_TAG1
   action drop
    count src_v4


Device# show sdwan from-vsmart policy
from-vsmart sla-class test_sla_class
 latency 50
from-vsmart app-route-policy test_app_route_policy
 vpn-list vpn_1_list
  sequence 1
   match
    destination-ip 10.2.3.21/32
   action
    sla-class test_sla_class
    sla-class strict
  sequence 2
   match
    destination-port 80
```

```
   action
    sla-class test_sla_class
    no sla-class strict
  sequence 3
   match
    destination-data-prefix-list test_data_prefix_list
   action
    sla-class test_sla_class
    sla-class strict

from-vsmart lists vpn-list vpn_1_list
 vpn 1
 vpn 102
from-vsmart lists data-prefix-list test_data_prefix_list
 ip-prefix 10.1.1.0/8


Device# show sdwan from-vsmart policy cflowd-template
from-vsmart cflowd-template test-cflowd-template
 flow-active-timeout   30
 flow-inactive-timeout 30
 template-refresh      30
 collector vpn 1 address 172.16.255.15 port 13322
Device# show sdwan from-vsmart policy cflowd-template collector
from-vsmart cflowd-template test-cflowd-template
 collector vpn 1 address 172.16.255.15 port 13322
```

show sdwan from-vsmart tag-instances

To display the tags downloaded from the Cisco SD-WAN Controller, use the **show sdwan from-vsmart tag-instances** command in privileged EXEC mode.

show sdwan from-vsmart tag-instances

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	This command was introduced.
Cisco IOS XE Catalyst SD-WAN Release 17.16.1a	This command is no longer supported. Use the **show sdwan tag-instances from-vsmart** command instead.

Usage Guidelines

Use the **show sdwan from-vsmart tag-instances** command to show user configuration of tag-instances.

Examples

The following is a sample output from **show sdwan from-vsmart tag-instances** command, displaying tags downloaded from Cisco SD-WAN Controller:

```
Device# show sdwan from-vsmart tag-instances
tag-instances-from-vsmart
 tag-instance APP_facebook_TAG9
  id       60000
  app-list apps_facebook
 tag-instance APP_office_TAG10
  id       70000
  app-list apps_ms apps_zoom
 tag-instance APP_webex_TAG8
  id       50000
  app-list apps_webex
 tag-instance DP_V4_TAG1
  id              10000
  data-prefix-list pfx1
 lists data-prefix-list multicast_pfx
  ip-prefix 224.0.0.0/8
 lists data-prefix-list pfx1
  ip-prefix 10.20.24.0/24
 lists app-list apps_facebook
  app dns
  app facebook
 lists app-list apps_ms
  app ms-office-365
  app ms-office-web-apps
  app ms-services
```

Related Commands

Command	Description
show sdwan from-vsmart policy	Displays policy downloaded from Cisco SD-WAN Controller.

show sdwan ftm umts

To view the Underlay Measurement and Tracing Services (UMTS) probes that are active on an Cisco Catalyst SD-WAN tunnel, use the **show sdwan ftm umts** command in privileged EXEC mode.

show sdwan ftm umts

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	This command was introduced.

Example

The following example shows UMTS probes that are active on the Cisco Catalyst SD-WAN tunnels.

This command displays a summary of tunnels configured for UMTS, and the corresponding trigger. The tunnels that are enabled for the on-demand option or for the events, are displayed only for a limited period because they are nonperiodic triggers.

```
Device#show sdwan ftm umts probes
MODE     TYPE       ACTIVE   VALID

CONFIG   MONITOR    1        1

CONFIG   SLA        1        1

CONFIG   PMTU       1        1

EXEC     MONITOR    0        0

EXEC     SLA        0        0

EXEC     PMTU       0        0

EXEC     ONDEMAND   0        0

Tunnel-Idx   Src IP       Dst IP       BFD LD    Color          Trigger              Periodic
 Timer left secs
13           10.1.14.14   10.1.15.15   20013     lte            PERIODIC             3575

14           10.1.14.14   10.0.21.16   20014     lte            PERIODIC             3575

15           10.1.14.14   10.0.111.1   20015     lte            PERIODIC             0

16           10.1.14.14   10.1.16.16   20016     lte            PERIODIC             3575

17           10.1.14.14   10.0.111.2   20017     lte            PERIODIC             0

18     10.1.14.14   10.0.5.11    20018      lte           PERIODIC             3
```

show sdwan ftm umts logs

To view the logs for event-driven or on-demand options of UMTS, use the **show sdwan ftm umts logs** command in privileged EXEC mode.

show sdwan ftm umts logs

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	This command was introduced.

Example

The following example displays the logs for event-driven or on-demand options of UMTS. The **show sdwan ftm umts logs** command displays the exact path traced by a Cisco IOS XE Catalyst SD-WAN

device on demand or for events. In some cases, the output is partial if the path has a large number of hops.

```
Device#show sdwan ftm umts logs
Showing 'UMTS' logs
=============================================================================================================
11     Mon Oct 31 21:26:18 2022:621  UMTS       (0   ) : ON_DEMAND Stream JSON: "vip_idx":
 "1","vip_time": "1667251578621","remote_color": "lte","local_color": "3g","remote_system_ip":
 "172.16.255.11","local_system_ip": "172.16.255.15","proto": "IPSEC","sent_qos": "72","state":
 "UP","event_type": "ON_DEMAND","event_subtype": "NONE","hops": {"ip": "10.0.20.23","ip":
"10.0.5.11"}
3      Mon Oct 31 21:26:49 2022:619  UMTS       (8   ) : ON_DEMAND Stream JSON: "vip_idx":
 "9","vip_time": "1667251609619","remote_color": "lte","local_color": "3g","remote_system_ip":
 "172.16.255.21","local_system_ip": "172.16.255.15","proto": "IPSEC","sent_qos": "72","state":
 "UP","event_type": "ON_DEMAND","event_subtype": "NONE","hops": {"ip": "10.0.20.23","ip":
"0.0.0.0","ip": "0.0.0.0","ip": "0.0.0.0","ip": "0.0.0.0","ip": "0.0.0.0","ip":
"0.0.0.0","ip": "0.0.0.0","ip": "0.0.0.0","ip": "0.0.0.0","ip": "0.0.0.0","ip":
"0.0.0.0","ip": "0.0.0.0","ip": "0.0.0.0","ip": "0.0.0.0","ip": "0.0.0.0","ip":
"0.0.0.0","ip": "0.0.0.0","ip": "0.0.0.0","ip": "0.0.0.0","ip": "0.0.0.0","ip":
"0.0.0.0","ip": "0.0.0.0","ip": "0.0.0.0","ip": "0.0.0.0","ip": "0.0.0.0","ip":
"0.0.0.0","ip": "0.0.0.0","ip": "0.0.0.0","ip": "0.0.0.0","ip": "0.0.0.0","ip": "0.0.0.0"}
=============================================================================================================
Idx     Date-Time:MilliSec            Log-type(Idx in log-type) :   Log-message
============================[NOTE: Read it from bottom to
top]=====================================
Displyed aggregated log cnt 37 from log-types
[ UMTS      ] Max cnt: 500   Agg cnt: 37    Rotated: NO  Curent index: 36
```

show sdwan geofence-status

To verify the geofencing status and configuration, use the **show sdwan geofence-status** command in privileged EXEC mode.

show sdwan geofence-status

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Use this command to display geofencing configuration and status.

Examples

The following example shows that geofencing is enabled and that the device location is valid and within the defined fence:

```
Device# show sdwan geofence-status
geofence-status
 Geofence Config Status =                  Geofencing-Enabled
```

```
Target Latitude =                          37.317342
Target Longitude =                         -122.218170
Geofence Range(in m) =                     100
Current Device Location Status =           Location-Valid
Current Latitude =                         37.317567
Current Longitude =                        -122.218170
Current Device Status =                    Within-defined-fence
Distance from target location(in m) =      30
Last updated device location timestamp =   2021-04-14T19:26:34+00:00
```

show sdwan interface color

To display the color description of TLOC, use the **show sdwan interface color** command in privileged EXEC mode.

show sdwan interface color

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco Catalyst SD-WAN Manager Release 20.18.1	This command was introduced.

This sample output shows the TLOC color description for different interfaces.

```
device# show sdwan interface color

Interface                           Color            Color Description
-------------------------------------------------------------------------------------------------------
GigabitEthernet0/0/0                gold             gold network
GigabitEthernet0/0/1                silver           silver network
GigabitEthernet0/0/2                bronze           bronze network
GigabitEthernet0/0/4                3g               3g network
GigabitEthernet0/0/6                lte              lte network
TenGigabitEthernet0/1/0             blue             blue network
TenGigabitEthernet0/1/2             mpls             mpls network
TenGigabitEthernet0/1/3             red              red network
```

show sdwan ipsec inbound-connections

To display information about the IPsec tunnels that originate on remote routers on Cisco IOS XE SD-WAN devices, use the **show sdwan ipsec inbound-connections** command in privileged EXEC mode.

show sdwan ipsec inbound-connections [*local-TLOC-address*]

Syntax Description

local-TLOC-address	(Optional) Displays information about IPsec tunnels that originate on remote routers to the specified local TLOC address.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Cisco IOS XE Catalyst SD-WAN devices can use the standards-based Internet Key Exchange (IKE) protocol when establishing IPsec tunnels between a device within the overlay network and a device that is external to the overlay network, such as a cloud-hosted service or a remote device.

IPsec provides confidentiality, data integrity, access control, and data source authentication for the traffic being exchanged over the IPsec tunnel.

This command can be used to display information about IPsec tunnels that originate on remote routers on Cisco IOS XE SD-WAN devices.

Example

The following example shows how to display information about IPsec tunnels that originate on remote routers on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan ipsec inbound-connections

SOURCE SOURCE DEST DEST REMOTE REMOTE LOCAL LOCAL NEGOTIATED
IP PORT IP PORT TLOC ADDRESS TLOC COLOR TLOC ADDRESS TLOC COLOR ENCRYPTION ALGORITHM TC
SPIs
--------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------------
-----
10.6.17.254 12346 10.3.6.2 12366 2.1.1.1 default 10.3.206.1 public-internet AES-GCM-256 8
10.6.18.254 12386 10.3.6.2 12366 2.1.1.2 default 10.3.206.1 public-internet AES-GCM-256 8
```

The following example shows how to display information about IPsec tunnels that originate on remote routers to the specified local TLOC address 10.3.206.1 on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan ipsec inbound-connections 10.3.206.1
SOURCE SOURCE DEST DEST REMOTE REMOTE LOCAL LOCAL NEGOTIATED
IP PORT IP PORT TLOC ADDRESS TLOC COLOR TLOC ADDRESS TLOC COLOR ENCRYPTION ALGORITHM TC
SPIs
--------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------------
-----
10.6.17.254 12346 10.3.6.2 12366 2.1.1.1 default 10.3.206.1 public-internet AES-GCM-256 8
10.6.18.254 12386 10.3.6.2 12366 2.1.1.2 default 10.3.206.1 public-internet AES-GCM-256 8
```

Related Commands

Command	Description
show sdwan ipsec local-sa	Displays security association information for the IPsec tunnels that have been created for local TLOCs.
show sdwan ipsec outbound-connections	Displays information about the IPsec tunnels to remote routers.

Command	Description
show sdwan ipsec pwk inbound-connections	Displays pairwise keys information about IPsec tunnels that originate on remote routers.
show sdwan ipsec pwk local-sa	Displays security association and pairwise keys information for the IPsec tunnels that have been created for local TLOCs.
show sdwan ipsec pwk outbound-connections	Displays pairwise keys information about the IPsec tunnels to remote routers.

show sdwan ipsec local-sa

To display information about the IPsec tunnels that originate on remote routers on Cisco IOS XE SD-WAN devices, use the **show sdwan ipsec local-sa** command in privileged EXEC mode.

show sdwan ipsec local-sa [*local-TLOC-address*]

Syntax Description

local-TLOC-address	(Optional) Displays security association information for the IPsec tunnels that have been created for the specified local TLOC address.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Cisco SD-WAN routers can use the standards-based Internet Key Exchange (IKE) protocol when establishing IPsec tunnels between a device within the overlay network and a device that is external to the overlay network, such as a cloud-hosted service or a remote device.

IPsec provides confidentiality, data integrity, access control, and data source authentication for the traffic being exchanged over the IPsec tunnel.

This command can be used to display security association information for the IPsec tunnels that have been created for local TLOCs on Cisco IOS XE SD-WAN devices.

Example

The following example shows how to display security association information for the IPsec tunnels that have been created for local TLOCs on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan ipsec local-sa

TLOC ADDRESS TLOC COLOR SPI IPv4 IPv6 PORT KEY HASH
------------------------------------------------------------------------------
10.3.206.1 public-internet 288 10.3.6.2 :: 12366 *****8415
10.3.206.1 public-internet 289 10.3.6.2 :: 12366 *****5c2c
```

The following example shows how to display security association information for the IPsec tunnels that have been created for the specified local TLOC address 10.3.206.1 on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan ipsec local-sa 10.3.206.1
SOURCE SOURCE DEST TLOC ADDRESS TLOC COLOR SPI IPv4 IPv6 PORT KEY HASH
------------------------------------------------------------------------------
10.3.206.1 public-internet 288 10.3.6.2 :: 12366 *****8415
10.3.206.1 public-internet 289 10.3.6.2 :: 12366 ***
```

Related Commands

Command	Description
show sdwan ipsec inbound-connections	Displays information about IPsec tunnels that originate on remote routers.
show sdwan ipsec outbound-connections	Displays information about the IPsec tunnels to remote routers.
show sdwan ipsec pwk inbound-connections	Displays pairwise keys information about IPsec tunnels that originate on remote routers.
show sdwan ipsec pwk local-sa	Displays security association and pairwise keys information for the IPsec tunnels that have been created for local TLOCs.
show sdwan ipsec pwk outbound-connections	Displays pairwise keys information about the IPsec tunnels to remote routers.

show sdwan ipsec outbound-connections

To view information about the IPsec tunnels to remote routers on Cisco IOS XE SD-WAN devices, use the **show sdwan ipsec outbound-connections** command in privileged EXEC mode.

show sdwan ipsec outbound-connections [*source-ip*]

Syntax Description

source-ip	(Optional) Displays information about the IPsec tunnels to remote routers for the specified source IP.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	The output of this command was modified. Starting from Cisco IOS XE Catalyst SD-WAN Release 17.6.1a, the command output replaces the `Authentication Used` column with the `Integrity Used` column. The values `null`, `ah-sha1-hmac`, `ah-no-id`, and `sha1-hmac` are replaced with `none`, `ip-udp-esp`, `ip-udp-esp-no-id`, and `esp` respectively.

Usage Guidelines

Cisco IOS XE Catalyst SD-WAN devices can use the standards-based Internet Key Exchange (IKE) protocol when establishing IPsec tunnels between a device within the overlay network and a device that is external to the overlay network, such as a cloud-hosted service or a remote device.

IPsec provides confidentiality, data integrity, access control, and data source authentication for the traffic being exchanged over the IPsec tunnel.

This command can be used to display information about the IPsec tunnels to remote routers on Cisco IOS XE SD-WAN devices.

Example

The following is a sample output of the **show sdwan ipsec outbound-connections** for Cisco IOS XE Catalyst SD-WAN Release 17.6.1a and later.

The following are sample outputs of the **show sdwan ipsec outbound-connections** command for releases prior to Cisco IOS XE Catalyst SD-WAN Release 17.6.1a.

The following example displays information about the IPsec tunnels to remote routers on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan ipsec outbound-connections

SOURCE SOURCE DEST DEST REMOTE REMOTE AUTHENTICATION NEGOTIATED
IP PORT IP PORT SPI TUNNEL MTU TLOC ADDRESS TLOC COLOR USED KEY HASH ENCRYPTION ALGORITHM
TC SPIs
--------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------------
-----------
10.64.0.18 12346 10.64.0.2 12366 256 1442 10.1.0.1 mpls AH_SHA1_HMAC *****c4cc AES-GCM-256
 8
10.64.0.18 12346 10.64.0.6 12366 256 1442 10.1.0.2 mpls AH_SHA1_HMAC *****5d57 AES-GCM-256
 8
10.64.0.18 12346 10.64.0.26 12366 256 1442 10.4.0.1 mpls AH_SHA1_HMAC *****e9b4 AES-GCM-256
 8
10.64.2.38 12346 10.64.2.6 17196 256 1442 10.4.0.1 biz-internet AH_SHA1_HMAC *****4ee7
AES-GCM-256 8
10.64.2.38 12346 10.64.2.26 12366 256 1442 10.1.0.1 biz-internet AH_SHA1_HMAC *****a094
AES-GCM-256 8
10.64.2.38 12346 10.64.2.30 12366 256 1442 10.1.0.2 biz-internet AH_SHA1_HMAC *****d092
AES-GCM-256 8
```

The following example shows how to display information about the IPsec tunnels to remote routers from the specified source IP 100.64.0.18 on Cisco IOS XE SD-WAN devices.

show sdwan ipsec pwk inbound-connections

To display pairwise keys information about the IPsec tunnels that originate on remote routers on Cisco IOS XE SD-WAN devices, use the **show sdwan ipsec pwk inbound-connections** command in privileged EXEC mode.

show sdwan ipsec pwk inbound-connections [*local-TLOC-address*]

Syntax Description

local-TLOC-address	(Optional) Displays pairwise keys information about the IPsec tunnels that originate on remote routers for the specified local TLOC address.

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Cisco IOS XE Catalyst SD-WAN devices can use the standards-based Internet Key Exchange (IKE) protocol when establishing IPsec tunnels between a device within the overlay network and a device that is external to the overlay network, such as a cloud-hosted service or a remote device.

IPsec provides confidentiality, data integrity, access control, and data source authentication for the traffic being exchanged over the IPsec tunnel.

IPsec pairwise keys feature implements controller-based key exchange protocol between device and controller. A pair of IPsec session keys (one encryption key and one decryption key) are configured per pair of local and remote Transport Locations (TLOC).

This command can be used to display pairwise keys information about the IPsec tunnels that originate on remote routers on Cisco IOS XE Catalyst SD-WAN devices.

Example

The following example shows how to display pairwise keys information about the IPsec tunnels that originate on remote routers on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan ipsec pwk inbound-connections

DEST        LOCAL            LOCAL            REMOTE           REMOTE
                SA    PKEY  NONCE   PKEY    SS   D-KEY   AH
              SOURCE IP                   PORT                   DEST IP
                   PORT     TLOC ADDRESS      TLOC COLOR      TLOC ADDRESS
      TLOC COLOR     PWK-SPI  INDEX    ID    HASH   HASH   HASH   HASH  AUTH
-----------------------------------------+--------+--------------------------
-------------+---------+---------------+---------------+---------------+---
-------------+---------+------+------+------+------+------+------+----
10.6.17.254                              12346    10.3.6.2
             12366    10.3.206.1       public-internet  2.1.1.1
default          000000   9      0                                    true

10.6.18.254                              12386    10.3.6.2
             12366    10.3.206.1       public-internet  2.1.1.2
default          000000   10     0                                    true
```

The following example shows how to display pairwise keys information about the IPsec tunnels that originate on remote routers for the specified local TLOC address 10.3.206.1 on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan ipsec pwk inbound-connections 10.3.206.1

DEST        LOCAL            LOCAL            REMOTE           REMOTE
      SA    PKEY  NONCE   PKEY    SS   D-KEY   AH
              SOURCE IP                   PORT                   DEST IP
             PORT     TLOC ADDRESS      TLOC COLOR      TLOC ADDRESS
TLOC COLOR     PWK-SPI  INDEX    ID    HASH   HASH   HASH   HASH  AUTH
-----------------------------------------+--------+--------------------------
-------------+--------+---------------+---------------+---------------+-
```

```
---------------+---------+------+------+------+------+------+------+----
10.6.17.254                              12346    10.3.6.2
                12366    10.3.206.1       public-internet  2.1.1.1
default           000000   9      0                                  true
10.6.18.254                              12386    10.3.6.2
                 12366    10.3.206.1       public-internet  2.1.1.2
default           000000   10     0                                  true
```

Related Commands

Command	Description
show sdwan ipsec inbound-connections	Displays information about IPsec tunnels that originate on remote routers.
show sdwan ipsec local-sa	Displays security association information for the IPsec tunnels that have been created for local TLOCs.
show sdwan ipsec outbound-connections	Displays information about the IPsec tunnels to remote routers.
show sdwan ipsec pwk local-sa	Displays security association and pairwise keys information for the IPsec tunnels that have been created for local TLOCs.
show sdwan ipsec pwk outbound-connections	Displays pairwise keys information about the IPsec tunnels to remote routers.

show sdwan ipsec pwk local-sa

To display security association and pairwise keys information for the IPsec tunnels that have been created for local TLOCs on Cisco IOS XE SD-WAN devices, use the **show sdwan ipsec pwk local-sa** command in privileged EXEC mode.

show sdwan ipsec pwk local-sa [*local-TLOC-address*]

Syntax Description

local-TLOC-address	(Optional) Displays security association and pairwise keys information for the IPsec tunnels that have been created for the specified local TLOC address

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Cisco IOS XE Catalyst SD-WAN devices can use the standards-based Internet Key Exchange (IKE) protocol when establishing IPsec tunnels between a device within the overlay network and a device that is external to the overlay network, such as a cloud-hosted service or a remote device.

IPsec provides confidentiality, data integrity, access control, and data source authentication for the traffic being exchanged over the IPsec tunnel.

IPsec Pairwise Keys feature implements controller-based key exchange protocol between device and controller. A pair of IPsec session keys (one encryption key and one decryption key) are configured per pair of local and remote Transport Locations (TLOC).

This command can be used to display security association and pairwise keys information for the IPsec tunnels that have been created for local TLOCs on Cisco IOS XE Catalyst SD-WAN devices.

Example

The following example shows how to display security association and pairwise keys information for the IPsec tunnels that have been created for local TLOCs on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan ipsec pwk local-sa

SOURCE           SA              PKEY      NONCE  PKEY TLOC-ADDRESS
TLOC-COLOR       SOURCE-IP  PORT   SPI  INDEX  ID   HASH  HASH
------------------------------------------------------------------------------
10.3.206.1   public-internet 10.3.6.2   12366  292  37     0
10.3.206.1   public-internet 10.3.6.2   12366  293  38     0
```

The following example shows how to display security association and pairwise keys information for the IPsec tunnels that have been created for local TLOCs from the specified source IP 10.3.206.1 on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan ipsec pwk local-sa 10.3.206.1

SOURCE      SA    PKEY  NONCE PKEY
TLOC-ADDRESS TLOC-COLOR      SOURCE-IP  PORT   SPI  INDEX  ID   HASH  HASH
------------------------------------------------------------------------------
10.3.206.1   public-internet 10.3.6.2   12366  292  37     0
10.3.206.1   public-internet 10.3.6.2   12366  293  38     0
```

Related Commands

Command	Description
show sdwan ipsec inbound-connections	Displays information about IPsec tunnels that originate on remote routers.
show sdwan ipsec local-sa	Displays security association information for the IPsec tunnels that have been created for local TLOCs.
show sdwan ipsec outbound-connections	Displays information about the IPsec tunnels to remote routers.
show sdwan ipsec pwk inbound-connections	Displays pairwise keys information about IPsec tunnels that originate on remote routers.
show sdwan ipsec pwk outbound-connections	Displays pairwise keys information about the IPsec tunnels to remote routers.

show sdwan ipsec pwk outbound-connections

To display pairwise keys information about the IPsec tunnels to remote routers on Cisco IOS XE SD-WAN devices, use the **show sdwan ipsec pwk outbound-connections** command in privileged EXEC mode.

show sdwan ipsec pwk outbound-connections [*source-ip*]

Syntax Description

source-ip	(Optional) Displays pairwise keys information about the IPsec tunnels to remote routers from the specified source IP.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Cisco IOS XE Catalyst SD-WAN devices can use the standards-based Internet Key Exchange (IKE) protocol when establishing IPsec tunnels between a device within the overlay network and a device that is external to the overlay network, such as a cloud-hosted service or a remote device.

IPsec provides confidentiality, data integrity, access control, and data source authentication for the traffic being exchanged over the IPsec tunnel.

IPsec Pairwise Keys feature implements controller-based key exchange protocol between device and controller. A pair of IPsec session keys (one encryption key and one decryption key) are configured per pair of local and remote Transport Locations (TLOC).

This command can be used to display pairwise keys information about the IPsec tunnels to remote routers on Cisco IOS XE SD-WAN devices.

Example

The following example shows how to display pairwise keys information about the IPsec tunnels to remote routers on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan ipsec pwk outbound-connections

SOURCE      DEST        LOCAL            LOCAL            REMOTE           REMOTE
         SA
PKEY  NONCE   PKEY    SS   E-KEY   AH
               SOURCE IP                    PORT                   DEST IP

PORT     TLOC ADDRESS      TLOC COLOR      TLOC ADDRESS      TLOC COLOR     PWK-SPI  INDEX

ID    HASH   HASH   HASH   HASH  AUTH
-------------------------------------+--------+-------------------------------------+-----
---+---------------+---------------+---------------+---------------+---------+------+------+
------+------+------+------+----
10.64.0.18                               12346    10.64.0.2
12366
10.3.0.1         mpls             10.1.0.1         mpls             000000   1      0
c4cc  true
10.64.0.18                               12346    10.64.0.6
12366
10.3.0.1         mpls             10.1.0.2         mpls             000000   3      0
5d57  true
10.64.0.18                               12346    10.64.0.26
12366
10.3.0.1         mpls             10.4.0.1         mpls             000000   5      0
```

```
e9b4  true
10.64.2.38                              12346    10.64.2.6
17196
10.3.0.1         biz-internet     10.4.0.1         biz-internet      000000   6      0
4ee7  true
10.64.2.38                              12346    10.64.2.26
12366
10.3.0.1         biz-internet     10.1.0.1         biz-internet      000000   2      0
a094  true
10.64.2.38                              12346    10.64.2.30
12366
10.3.0.1         biz-internet     10.1.0.2         biz-internet      000000   4      0
d092  true
```

The following example shows how to display pairwise keys information about the IPsec tunnels to remote routers from the specified source IP 10.64.0.18 on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan ipsec pwk outbound-connections 10.3.206.1

SOURCE    DEST        LOCAL            LOCAL      REMOTE     REMOTE
SA    PKEY  NONCE   PKEY    SS   E-KEY   AH    SOURCE IP     PORT
DEST IP    PORT   TLOC ADDRESS      TLOC COLOR      TLOC ADDRESS      TLOC COLOR
PWK-SPI  INDEX    ID    HASH HASH   HASH   HASH  AUTH
-----------------------------------------+--------+-------------------------------
-+---------------+----------------+---------------+---------------+---------+--
--+------+------+------+----
10.64.0.18                         12346    10.64.0.2                          12366
10.3.0.1         mpls              10.1.0.1         mpls  00000   1      0   c4cc  true
10.64.0.18                         12346    10.64.0.6                          12366
10.3.0.1         mpls              10.1.0.2         mpls              000000   3      0
5d57  true
```

Related Commands

Command	Description
show sdwan ipsec inbound-connections	Displays information about IPsec tunnels that originate on remote routers.
show sdwan ipsec local-sa	Displays security association information for the IPsec tunnels that have been created for local TLOCs.
show sdwan ipsec outbound-connections	Displays information about the IPsec tunnels to remote routers.
show sdwan ipsec pwk inbound-connections	Displays pairwise keys information about IPsec tunnels that originate on remote routers.
show sdwan ipsec pwk local-sa	Displays security association and pairwise keys information for the IPsec tunnels that have been created for local TLOCs.

show sdwan nat-fwd ip-nat-translation

To display active NAT translations on Cisco IOS XE SD-WAN devices, use the **show sdwan nat-fwd ip-nat-translation** command in privileged EXEC mode.

show sdwan nat-fwd ip-nat-translation

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines NAT enables private IP internetworks that use nonregistered IP addresses to connect to the internet. NAT operates on a device, usually connecting two networks. Before packets are forwarded onto another network, NAT translates the private (not globally unique) addresses in the internal network into legal addresses.

This command can be used to display active NAT translations on Cisco IOS XE SD-WAN devices.

Example

The following example shows how to display active NAT translations on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan nat-fwd ip-nat-translation
nat-fwd ip-nat-translation 10.3.40.14 168.61.161.212 62244 443 3 6
 inside-global-addr  100.64.2.38
 outside-global-addr 168.61.161.212
 inside-global-port  5841
 outside-global-port 443
 flags               536887296
 application-type    0
nat-fwd ip-nat-translation 10.3.40.14 52.255.188.83 62246 443 3 6
 inside-global-addr  100.64.2.38
 outside-global-addr 52.255.188.83
 inside-global-port  5844
 outside-global-port 443
 flags               2113552
 application-type    0
```

Related Commands

Command	Description
show sdwan nat-fwd ip-nat-translation-verbose	Displays detailed active NAT translations.

show sdwan nat-fwd ip-nat-translation-verbose

To display detailed active NAT translations on Cisco IOS XE SD-WAN devices, use the **show sdwan nat-fwd ip-nat-translation-verbose** command in privileged EXEC mode.

show sdwan nat-fwd ip-nat-translation-verbose

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines NAT enables private IP internetworks that use nonregistered IP addresses to connect to the internet. NAT operates on a device, usually connecting two networks. Before packets are forwarded onto another network, NAT translates the private (not globally unique) addresses in the internal network into legal addresses.

This command can be used to display detailed active NAT translations on Cisco IOS XE Catalyst SD-WAN devices.

Example

The following example shows how to display detailed active NAT translations on Cisco IOS XE Catalyst SD-WAN devices.

```
Device# show sdwan nat-fwd ip-nat-translation-verbose

nat-fwd ip-nat-translation-verbose 10.3.40.10 198.18.1.222 43965 80 3 6
 inside-global-addr  100.64.2.38
 outside-global-addr 198.18.1.222
 inside-global-port  5280
 outside-global-port 80
 flags               1075855376
 application-type    0
 entry-id            0xea5bc6c0
 in_mapping_id       1
 out_mapping_id      0
 create_time         "Thu Dec  3 19:37:07 2020"
 last_used_time      "Thu Dec  3 19:37:59 2020"
 pkts_in             13
 pkts_out            11
 timeout             "13 seconds"
 usecount            1
 input-idb           GigabitEthernet7
 output-idb          GigabitEthernet4
 bytes_in            638
 bytes_out           11335
```

Related Commands

Command	Description
show sdwan nat-fwd ip-nat translation	Displays active NAT translations.

show sdwan omp cloudexpress

To display the available routes from each gateway device in the network, for each application configured in Cloud onRamp for SaaS, use the **show sdwan omp cloudexpress** command in privileged EXEC mode.

show sdwan omp cloudexpress

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command is supported for Cisco Catalyst SD-WAN.

Usage Guidelines

The command displays the available routes from each gateway device in the network, for each application configured in Cloud onRamp for SaaS. Cloud onRamp for SaaS sends the routes, together with service level agreement (SLA) information to the devices in the network to use to determine the best path, to the cloud server for the application. The path may be through direct internet access (DIA) or through a gateway device.

The APP ID column indicates the application, using the following codes:

APP ID	Application
1	Salesforce
2	Office 365
3	Amazon AWS
4	Oracle
6	Box
7	Dropbox
9	Intuit
10	Concur
11	Sugar CRM
12	Zoho CRM
13	Zendesk
14	GoToMeeting
15	Webex
16	Google

The STATUS column codes are as follows:

Status	Description
C	Chosen
I	Installed
Red	Redistributed
Rej	Rejected

Status	Description
L	Looped
R	Resolved
S	Stale
Ext	Extranet
Inv	Invalid

Examples

The following is an example output for the **show sdwan omp cloudexpress** command:

```
Device#show sdwan omp cloudexpress
                     APP  APP   SUBAPP
VPN  ORIGINATOR      ID   TYPE  ID      APP NAME    FROM PEER      STATUS
-------------------------------------------------------------------------
1    172.16.255.15   3    2     0       amazon_aws  172.16.255.15  C,R
                                                   172.16.255.20  C,R
1    172.16.255.15   15   4     8       webex       172.16.255.15  C,R
                                                   172.16.255.20  C,R
1    172.16.255.16   3    0     0       amazon_aws  172.16.255.16  C,R
                                                   172.16.255.20  C,R
```

show sdwan omp ipv6-routes

To display IPv6 OMP routes on Cisco IOS XE Catalyst SD-WAN devices, use the **show sdwan omp ipv6-routes** command in privileged EXEC mode.

show sdwan omp ipv6-routes [*WORD*]

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

On Cisco Catalyst SD-WAN devices, OMP advertises to its peers the routes and services that it has learned from its local site, along with their corresponding transport location mappings, which are called TLOCs.

OMP routes carry information that the device learns from the routing protocols running on its local network including routes learned from BGP and OSPF as well direct, connected, and static routes. This command can be used to display IPv6 OMP routes on Cisco IOS XE Catalyst SD-WAN devices.

Example

The following example shows how to display IPv6 OMP routes on Cisco IOS XE Catalyst SD-WAN devices.

```
Device# show sdwan omp ipv6-routes
------------------------------------------------
omp route entries for vpn 10 route 2001:db8:1::/64
------------------------------------------------
           RECEIVED FROM:
peer            0.0.0.0
path-id         66
label           1002
status          C,Red,R
loss-reason     not set
lost-to-peer    not set
lost-to-path-id not set
    Attributes:
     originator       10.3.0.2
     type             installed
     tloc             10.3.0.2, mpls, ipsec
     ultimate-tloc    not set
     domain-id        not set
     overlay-id        1
     site-id          300
     preference       not set
     tag              not set
     origin-proto     connected
     origin-metric    0
     as-path          not set
     unknown-attr-len not set
           RECEIVED FROM:
peer            0.0.0.0
path-id         68
label           1002
status          C,Red,R
loss-reason     not set
lost-to-peer    not set
lost-to-path-id not set
    Attributes:
     originator       10.3.0.2
     type             installed
     tloc             10.3.0.2, biz-internet, ipsec
     ultimate-tloc    not set
     domain-id        not set
     overlay-id        1
     site-id          300
     preference       not set
     tag              not set
     origin-proto     connected
     origin-metric    0
     as-path          not set
     unknown-attr-len not set
           ADVERTISED TO:
peer    12.12.12.12
           ADVERTISED TO:
peer    22.22.22.22
```

Related Commands

Commands	Description
show sdwan omp cloudexpress	Displays OMP routes for applications configured with Cloud OnRamp for SaaS.
show sdwan omp milticast-auto-discover	Displays the peers that support multicast.
show sdwan omp multicast-routes	Displays the multicast routes that OMP has learned from PIM join messages.
show sdwan omp peers	Displays information about the OMP peering sessions that are active on the local Cisco Catalyst SD-WAN devices.
show sdwan omp routes	Displays information about OMP routes.
show sdwan omp services	Displays the services learned from OMP peering sessions.
show sdwan omp summary	Displays information about the OMP sessions running between Cisco Catalyst SD-WAN devices.
show sdwan omp tlocs-paths	Displays information about the TLOC path information.
show sdwan omp tlocs	Displays information learned from the TLOC routes advertised over the OMP sessions running between Cisco Catalyst SD-WAN devices.

show sdwan omp multicast-auto-discover

show sdwan omp multicast-auto-discover—List the peers that support multicast on Cisco IOS XE Catalyst SD-WAN device and vSmart controllers only.

Command Syntax

show sdwan omp multicast-auto-discover [**detail**]

Syntax Description

	None: List standard information about the OMP Multicast routes.
detail	Detailed Information: List detailed information.

Output Fields

The output fields are self-explanatory.

Command History

Release	Modification
17.2.1	Command introduced.

Example

```
Device# show sdwan omp multicast-auto-discover
Code:
C   -> chosen
I   -> installed
Red -> redistributed
Rej -> rejected
L   -> looped
R   -> resolved
S   -> stale
Ext -> extranet
Inv -> invalid

ADDRESS        SOURCE
FAMILY   VPN  ORIGINATOR     FROM PEER      STATUS
-----------------------------------------------------
ipv4     1    172.16.255.11  172.16.255.19  C,I,R
                             172.16.255.20  C,I,R
         1    172.16.255.14  172.16.255.19  C,I,R
                             172.16.255.20  C,I,R
         1    172.16.255.15  172.16.255.19  C,I,R
                             172.16.255.20  C,I,R
         1    172.16.255.16  0.0.0.0        C,Red,R
         1    172.16.255.21  172.16.255.19  C,I,R
                             172.16.255.20  C,I,R
```

show sdwan omp multicast-routes

show sdwan omp multicast-routes—List the multicast routes that OMP has learned from PIM join messages (on Cisco IOS XE Catalyst SD-WAN device and vSmart controllers).

Command Syntax

show sdwan omp multicast-routes [**detail**]

Syntax Description

	None: List standard information about Cisco IOS XE Catalyst SD-WAN devices supporting multicast routes.
detail	Detailed Information: List detailed information.

Output Fields

The output fields are self-explanatory.

Command History

Release	Modification
17.2.1	Command introduced.

Example

```
Device# show sdwan omp multicast-routes
Code:
C   -> chosen
I   -> installed
Red -> redistributed
Rej -> rejected
L   -> looped
R   -> resolved
S   -> stale
Ext -> extranet
Inv -> invalid

ADDRESS              SOURCE
FAMILY   TYPE   VPN  ORIGINATOR     DESTINATION    GROUP      SOURCE   FROM PEER      RP           STATUS
-------------------------------------------------------------------------------------------------------
ipv4     (*,G)  1    172.16.255.14  172.16.255.16  225.0.0.1  0.0.0.0  172.16.255.19  10.20.25.18  C,I,R
                                                                       172.16.255.20  10.20.25.18  C,I,R
```

show sdwan omp peers

To display information about OMP peers on Cisco SD-WAN Controllers and Cisco IOS XE Catalyst SD-WAN devices, use the **show sdwan omp peers** command in privileged EXEC mode.

Command Syntax

show sdwan omp peers [**detail**]

Syntax Description

	None: List information about all OMP peering sessions on the local device.
detail	Detailed information: Display detailed information.

Output Fields

Field	Explanation
Domain ID	Identifier of the domain that the device is a member of.
downcount	Number of times an OMP peering session has gone down.

Field	Explanation
last-downtime	The last time that an OMP peering session went down.
last-uptime	The last time that an OMP peering session came up.
Peer or peer	IP address of the connected Cisco IOS XE Catalyst SD-WAN device.
Region ID	Region assigned for Hierarchical SD-WAN. For information, see Hierarchical SD-WAN.
R/I/S	Number of routes received, installed, and sent over the OMP session.
routes-installed	Number of routes installed over the OMP session.
routes-received	Number of routes received over the OMP session.
routes-sent	Number of routes sent over the OMP session.
services-installed	Number of services installed that were learned over OMP sessions.
services-received	Number of services received over OMP sessions.
services-sent	Number of services advertised over OMP sessions.
Site ID	Identifier of the Cisco IOS XE Catalyst SD-WAN device administrative site where the connected Cisco IOS XE Catalyst SD-WAN device is located.
state	Operational state of the connection to the Cisco IOS XE Catalyst SD-WAN device: • down—The connection is not functioning. • down-in-gr—A connection on which OMP grace restart is enabled is down. init—The connection is initializing. up—The connection is operating.
tlocs-installed	Number of TLOCs installed that were learned over OMP sessions.
tlocs-received	Number of TLOCs received over OMP sessions.
tlocs-sent	Number of TLOCs advertised over OMP sessions.
Type or type	Type of Cisco IOS XE Catalyst SD-WAN device • Cisco IOS XE Catalyst SD-WAN device • vsmart - vSmart controller

Field	Explanation
upcount	Number of times an OMP peering session has come up.
Uptime	How long the OMP session between the Cisco IOS XE Catalyst SD-WAN devices has been up and operational.

Command History

Release	Modification
16.12.1	Command introduced.
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	Added the Region ID column to the command output.

Examples

Example 1

```
Device# show sdwan omp peers
R -> routes received
I -> routes installed
S -> routes sent

                        DOMAIN    SITE
PEER             TYPE   ID        ID        STATE    UPTIME           R/I/S
-----------------------------------------------------------------------------
172.16.255.19    vsmart  1         100       up       0:04:09:59       7/7/3
172.16.255.20    vsmart  1         200       up       0:04:10:14       7/0/3

vEdge# show omp peers 172.16.255.19 detail

peer                     172.16.255.19
type                     vsmart
domain-id                1
site-id                  100
state                    up
version                  1
legit                    yes
upcount                  1
downcount                0
last-uptime              2014-11-12T14:52:19+00:00
last-downtime            0000-00-00T00:00:00+00:00
uptime                   0:04:12:30
hold-time                15
graceful-restart         supported
graceful-restart-interval 300
hello-sent               3032
hello-received           3030
handshake-sent           1
handshake-received       1
alert-sent               0
alert-received           0
inform-sent              5
inform-received          5
update-sent              8
update-received          27
policy-sent
```

```
policy-received
total-packets-sent        3046
total-packets-received    3063
routes-received           7
routes-installed          7
routes-sent               3
tlocs-received            4
tlocs-installed           4
tlocs-sent                1
services-received         0
services-installed        0
services-sent             1
mcast-routes-received     0
mcast-routes-installed    0
mcast-routes-sent         0
```

Example 2

```
vSmart# show sdwan omp peers
R -> routes received
I -> routes installed
S -> routes sent
                        DOMAIN    SITE
PEER             TYPE   ID        ID        STATE    UPTIME           R/I/S
-------------------------------------------------------------------------------
172.16.255.11    vedge  1         100       up       0:00:38:20       3/0/9
172.16.255.14    vedge  1         400       up       0:00:38:22       0/0/11
172.16.255.15    vedge  1         500       up       0:00:38:22       3/0/8
172.16.255.16    vedge  1         600       up       0:00:38:21       4/0/7
172.16.255.20    vsmart 1         200       up       0:00:38:24       11/0/11
172.16.255.21    vedge  1         100       up       0:00:38:20       3/0/9
```

Example 3

```
vSmart# show sdwan omp peers
R -> routes received
I -> routes installed
S -> routes sent

                        DOMAIN    SITE
PEER             TYPE   ID        ID        STATE     UPTIME           R/I/S
-------------------------------------------------------------------------------
172.16.255.11    vedge  1         100       up        0:05:19:17       3/0/5
172.16.255.14    vedge  1         400       up        0:05:19:17       0/0/7
172.16.255.15    vedge  1         500       down-in-gr                 3/0/0
172.16.255.16    vedge  1         600       down                       0/0/0
172.16.255.20    vsmart 1         200       up        0:05:19:21       7/0/7
172.16.255.21    vedge  1         100       up        0:05:19:20       3/0/5
```

Example 4

Beginning with Cisco IOS XE Catalyst SD-WAN Release 17.7.1a, the command output includes the Region ID column.

```
Device# show sdwan omp peers
R -> routes received
I -> routes installed
S -> routes sent

TENANT                          DOMAIN    OVERLAY   SITE      REGION
ID       PEER            TYPE   ID        ID        ID        ID       STATE    UPTIME           R/I/S
-------------------------------------------------------------------------------------------------------
0        172.24.121.10   vsmart 1         1         100       0        up       12:04:39:41      32/28/16
0        172.24.122.10   vsmart 1         1         200       2        up       0:09:36:45       12/10/32
0        172.24.123.10   vsmart 1         1         300       2        up       12:04:44:52      12/0/32
0        172.24.124.10   vsmart 1         1         400       0        up       12:04:39:41      32/0/16
```

show sdwan omp routes

To display information about OMP routes on Cisco Catalyst SD-WAN Controllers and Cisco IOS XE Catalyst SD-WAN devices, use the command **show sdwan omp routes** in the privileged EXEC mode. OMP routes carry information that the device learns from the routing protocols running on its local network, including routes learned from BGP and OSPF, as well as direct, connected, and static routes.

Command Syntax

show sdwan omp routes *prefix address/length* [**family** *family address*] [**vpn** *vpn-id*] [**tenant** *tenant-id*] [**verify**] [**detail**]

show sdwan omp routes **tenant** *tenant-id* **vpn** *vpn-id prefix address* [**verify**] [**detail**]

Syntax Description

None	Lists the routing information about all OMP peering sessions on the local device.
prefix address	Displays the ip address prefix. Lists OMP route information for the specified route prefix.
length	Displays the route length. Lists OMP route information for the specified route prefix.
family *family address*	Displays the family. Lists OMP route information for the specified IP family.
vpn *vpn-id*	Displays VPN-specific routes. Lists the OMP routes for the specified VPN.
tenant *tenant-id*	Displays tenant ID. Specify tenant-id value within the range, 0 to 65534.
verify	Displays end-to-end verification information of a prefix availability, while keeping track of received and installed prefixes into RIB and FIB, TLOCs, and BFD sessions established.
detail	Displays detailed output information.

Output Fields

The output fields are self-explanatory.

Command Default NA

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 17.2	This command is introduced.
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	Added **REGION ID** to the output to show the Hierarchical SD-WAN region ID. Added **TENANT ID** to the output to show the tenant ID.
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	Added **PREFERENCE** and **AFFINITY GROUP NUMBER** to the output to indicate the affinity group preference order and the affinity ID.
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	Added **VERIFY** to the output to verify the OMP routes.
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	Added Multi-Region Fabric subregion information to the output. For information about subregions, see the Cisco SD-WAN Multi-Region Fabric (also Hierarchical SD-WAN) Configuration Guide.

Usage Guidelines

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.18.x, Cisco IOS XE Catalyst SD-WAN Release 17.15.2, and Cisco IOS XE Catalyst SD-WAN Release 17.12.5a, the **show sdwan omp routes** command requires specifying both the **tenant** *tenant-id* and **vpn** *vpn-id* when used with a prefix address.

Examples

In the following sample output, the **Region ID** column indicates either **1** for region 1, or **1.5** for subregion 5 of region 1.

```
Device#show sdwan omp routes

                  AFFINITY                                  PATH                    ATTRIBUTE
                  GROUP
TENANT VPN   PREFIX        FROM PEER  ID     LABEL STATUS    TYPE       TLOC IP    COLOR
ENCAP  PREFERENCE  NUMBER    REGION ID   REGION PATH
------------------------------------------------------------------------------------------------
0      1    10.1.1.0/24  0.0.0.0    70     1003  C,Red,R   installed  192.0.5.0  lte
ipsec  -           None       1.5         1
                         0.0.0.0    71     1003  C,Red,R   installed  192.0.5.0  3g
ipsec  -           None       1.5         1
                         0.0.0.0    72     1003  C,Red,R   installed  192.0.5.0  red
ipsec  -           None       1.5         1
0      1    10.1.2.0/24  192.0.2.0  2      1003  C,I,R     installed  192.0.6.0  lte
ipsec  -           None       1.5         1
                         192.0.2.0  4      1003  C,I,R     installed  192.0.6.0  3g
ipsec  -           None       1.5         1
                         192.0.2.0  5      1003  C,I,R     installed  192.0.6.0  red
ipsec  -           None       1.5         1
                         192.0.3.0  1      1003  C,R       installed  192.0.6.0  lte
ipsec  -           None       1.5         1
                         192.0.3.0  3      1003  C,R       installed  192.0.6.0  3g
ipsec  -           None       1.5         1
                         192.0.3.0  6      1003  C,R       installed  192.0.6.0  red
ipsec  -           None       1.5         1
0      1    10.1.3.0/24  192.0.2.0  35     1003  C,I,R     installed  192.0.7.0  lte
ipsec  -           None       1           1
```

```
                        192.0.2.0  36     1003  C,I,R     installed  192.0.7.0  3g
ipsec  -           None      1           1
                        192.0.3.0  35     1003  C,R       installed  192.0.7.0  lte
ipsec  -           None      1           1
                        192.0.3.0  36     1003  C,R       installed  192.0.7.0  3g
ipsec  -           None      1           1


Device# show sdwan omp routes

Code:
C -> chosen
I -> installed
Red -> redistributed
Rej -> rejected
L -> looped
R -> resolved
S -> stale
Ext -> extranet
Inv -> invalid
Stg -> staged
U -> TLOC unresolved
                                                PATH                    ATTRIBUTE
VPN    PREFIX              FROM PEER            ID     LABEL    STATUS    TYPE       TLOC IP
       COLOR            ENCAP  PREFERENCE
--------------------------------------------------------------------------------------------
1      192.0.2.0/24        192.168.1.3      1      1001     C,I,R     installed  192.168.1.152
    biz-internet     ipsec  -
202    192.0.2.1/24        192.168.1.3      2      1002     C,I,R     installed  192.168.1.152
    biz-internet     ipsec  -
202    192.0.2.0/24        0.0.0.0          68     1002     C,Red,R   installed  192.168.1.121
    biz-internet     ipsec  -

Device# show sdwan omp routes vpn 202 192.0.2.0/24
-------------------------------------------------
omp route entries for vpn 202 route 192.0.2.0/24
-------------------------------------------------
           RECEIVED FROM:
peer            0.0.0.0
path-id         68
label           1002
status          C,Red,R
loss-reason     not set
lost-to-peer    not set
lost-to-path-id not set
    Attributes:
     originator       192.168.1.121
     type             installed
     tloc             192.168.1.121, biz-internet, ipsec
     domain-id        not set
     site-id          121
     overlay-id        1
     preference       not set
     tag              not set
     origin-proto     connected
     origin-metric    0
     as-path          not set
     unknown-attr-len not set
           ADVERTISED TO:
peer    192.168.1.3
advertise-id    68
    Attributes:
     originator       192.168.1.121
     label            1002
     path-id          68
```

```
     tloc             192.168.1.121, biz-internet, ipsec
     domain-id        not set
     site-id          121
     overlay-id        1
     preference       not set
     tag              not set
     origin-proto     connected
     origin-metric    0
     as-path          not set
     unknown-attr-len not set
```

```
Device# show sdwan omp routes vpn 202
------------------------------------------------
omp route entries for vpn 202 route 192.0.2.1/24
------------------------------------------------
            RECEIVED FROM:
peer            0.0.0.0
path-id         68
label           1002
status          C,Red,R
loss-reason     not set
lost-to-peer    not set
lost-to-path-id not set
    Attributes:
     originator       192.168.1.121
     type             installed
     tloc             192.168.1.121, biz-internet, ipsec
     ultimate-tloc    not set
     domain-id        not set
     overlay-id        1
     site-id          121
     preference       not set
     tag              not set
     origin-proto     connected
     origin-metric    0
     as-path          not set
     unknown-attr-len not set
            ADVERTISED TO:
peer    192.168.1.3
    Attributes:
     originator       192.168.1.121
     label            1002
     path-id          68
     tloc             192.168.1.121, biz-internet, ipsec
     ultimate-tloc    not set
     domain-id        not set
     site-id          121
     overlay-id        1
     preference       not set
     tag              not set
     origin-proto     connected
     origin-metric    0
     as-path          not set
     unknown-attr-len not set
```

```
Device# show sdwan omp tenant 0 vpn 1 10.20.24.0/24 verify
-------------------------------------------------------------------------------
omp route entries for tenant-id 0 vpn 1 route 10.20.24.0/24
-------------------------------------------------------------------------------
            RECEIVED FROM:
peer            172.16.255.19
path-id         780
label           1003
status          C,I,R
loss-reason     not set
```

```
lost-to-peer    not set
lost-to-path-id not set
    Attributes:
     originator       172.16.255.15
     type             installed
     tloc             172.16.255.15, lte, ipsec
     ultimate-tloc    not set
     domain-id        not set
     overlay-id        1
     site-id          500
     preference       not set
     affinity-group  None
     region-id        None
     region-path      not set
     route-reoriginator      not set
     tag              not set
     origin-proto     connected
     origin-metric    0
     as-path          not set
     community        not set
     unknown-attr-len not set
     tloc-status      C,I,R
     bfd-status       up
     rib-status       rib-installed
           RECEIVED FROM:
peer            172.16.255.20
path-id         119
label           1003
status          C,R
loss-reason     not set
lost-to-peer    not set
lost-to-path-id not set
    Attributes:
     originator       172.16.255.15
     type             installed
     tloc             172.16.255.15, lte, ipsec
     ultimate-tloc    not set
     domain-id        not set
     overlay-id        1
     site-id          500
     preference       not set
     affinity-group  None
     region-id        None
     region-path      not set
     route-reoriginator      not set
     tag              not set
     origin-proto     connected
     origin-metric    0
     as-path          not set
     community        not set
     unknown-attr-len not set
     tloc-status      C,R
    bfd-status       up
     rib-status       rib-not-installed
```

```
Device# show sdwan omp routes tenant 0 vpn 1 10.2.2.0

Generating output, this might take time, please wait ...
Code:
C -> chosen
I -> installed
Red -> redistributed
Rej -> rejected
L -> looped
R -> resolved
```

```
S -> stale
Ext -> extranet
Inv -> invalid
Stg -> staged
IA -> On-demand inactive
U -> TLOC unresolved
BR-R -> Border-Router reoriginated
TGW-R -> Transport-Gateway reoriginated
R-TGW-R -> Reoriginated Transport-Gateway reoriginated
DERIVED
AFFINITY AFFINITY
PATH PSEUDO
GROUP GROUP
FROM PEER ID LABEL STATUS KEY TLOC IP COLOR
ENCAP PREFERENCE NUMBER NUMBER
--------------------------------------------------------------------------------
------------------------------------------------
12.16.255.20 1 1003 C,I,R 1 10.2.1.25 publicinternet
ipsec - None None
12.16.255.20 2 1003 C,I,R 1 10.2.1.25 lte
ipsec - None None
12.16.255.20 3 1003 C,I,R 1 10.2.1.25 gold
ipsec - None None
12.16.255.20 4 1003 C,I,R 1 10.2.1.25 silver
ipsec - None None
12.16.255.20 5 1003 C,I,R 1 10.2.1.25
```

show sdwan omp l2-routes

To display OMP L2VPN routes on a Cisco Catalyst SD-WAN Controller and Cisco IOS XE Catalyst SD-WAN device, use the command **show sdwan omp l2-routes** in the privileged EXEC mode.

Command Syntax

show sdwan omp l2-routes [**vpn** *vpn-id*] [**vc** *vc-id*]

Syntax Description

vpn *vpn-id*	Displays L2VPN-specific routes. Lists the OMP routes for the specified L2VPN.
vc *vc-id*	Displays Virtual Circuit (VC) ID that is used to identify a particular bridge domain. Specify bridge-domain vc-id value. Range: 1 to 4294967295

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.14.1a	This command is introduced.

Usage Guidelines

These commands are only used on Cisco Catalyst SD-WAN Controllers and Cisco IOS XE Catalyst SD-WAN devices.

Examples

The following shows a sample output of OMP information on Cisco IOS XE Catalyst SD-WAN devices:

```
Device# show sdwan omp l2-routes

Code:
C   -> chosen
I   -> installed
Red -> redistributed
Rej -> rejected
L   -> looped
R   -> resolved
S   -> stale
Ext -> extranet
Inv -> invalid
Stg -> staged
IA  -> On-demand inactive
U   -> TLOC unresolved

                                                REMOTE
                                     ROUTE                    IP                    SITE
                PATH                     SITE
VPN     VC ID         ORIGINATOR       TYPE   MAC ADDRESS      ADDRESS  VPN TYPE    ID
FROM PEER         ID     LABEL    STATUS    ID
-------------------------------------------------------------------------------------------
12      12            172.16.255.15    vpn    0000.0000.0000   ::       p2p         500
0.0.0.0           66     1004     C,Red,R   501

0.0.0.0           69     1004     C,Red,R   501
12      12            172.16.255.27    vpn    0000.0000.0000   ::       p2p         501
172.16.255.19     2      1014     C,I,R     500

172.16.255.20     1      1014     C,R       500
13      13            172.16.255.15    vpn    0000.0000.0000   ::       multipoint  500
0.0.0.0           66     1006     C,Red,R   -

0.0.0.0           69     1006     C,Red,R   -
13      13            172.16.255.27    vpn    0000.0000.0000   ::       multipoint  501
172.16.255.19     2      1016     C,I,R     -

172.16.255.20     1      1016     C,R       -
13      13            172.16.255.32    vpn    0000.0000.0000   ::       multipoint  503
172.16.255.19     1      1007     C,I,R     -

172.16.255.20     1      1007     C,R       -
15      1             172.16.255.15    vpn    0000.0000.0000   ::       p2p         500
0.0.0.0           66     1020     C,Red,R   501

0.0.0.0           69     1020     C,Red,R   501
```

```
15     1            172.16.255.27    vpn    0000.0000.0000   ::       p2p          501
172.16.255.19    2      1020     C,I,R     500

172.16.255.20    1      1020     C,R       500
```

```
Device# show sdwan omp l2-routes vpn 13

Code:
C   -> chosen
I   -> installed
Red -> redistributed
Rej -> rejected
L   -> looped
R   -> resolved
S   -> stale
Ext -> extranet
Inv -> invalid
Stg -> staged
IA  -> On-demand inactive
U   -> TLOC unresolved
                                                                    REMOTE
                                    ROUTE                   IP                   SITE
               PATH                     SITE
VPN    VC ID        ORIGINATOR       TYPE   MAC ADDRESS      ADDRESS  VPN TYPE    ID
FROM PEER        ID     LABEL    STATUS    ID
------------------------------------------------------------------------------------------
13     13           172.16.255.15    vpn    0000.0000.0000   ::       multipoint  500
0.0.0.0          66     1006     C,Red,R   -

0.0.0.0          69     1006     C,Red,R   -
13     13           172.16.255.27    vpn    0000.0000.0000   ::       multipoint  501
172.16.255.19    2      1016     C,I,R     -

172.16.255.20    1      1016     C,R       -
13     13           172.16.255.32    vpn    0000.0000.0000   ::       multipoint  503
172.16.255.19    1      1007     C,I,R     -

172.16.255.20    1      1007     C,R       -
```

```
Device# show sdwan omp l2-routes vpn 13 vc-id 13

Code:
C   -> chosen
I   -> installed
Red -> redistributed
Rej -> rejected
L   -> looped
R   -> resolved
S   -> stale
Ext -> extranet
Inv -> invalid
Stg -> staged
IA  -> On-demand inactive
U   -> TLOC unresolved
                                                                    REMOTE
                                    ROUTE                   IP                   SITE
               PATH                     SITE
VPN    VC ID        ORIGINATOR       TYPE   MAC ADDRESS      ADDRESS  VPN TYPE    ID
FROM PEER        ID     LABEL    STATUS    ID
------------------------------------------------------------------------------------------
13     13           172.16.255.15    vpn    0000.0000.0000   ::       multipoint  500
0.0.0.0          66     1006     C,Red,R   -

0.0.0.0          69     1006     C,Red,R   -
13     13           172.16.255.27    vpn    0000.0000.0000   ::       multipoint  501
```

```
172.16.255.19    2      1016     C,I,R     -

172.16.255.20    1      1016     C,R       -
13     13           172.16.255.32    vpn    0000.0000.0000   ::       multipoint  503
172.16.255.19    1      1007     C,I,R     -

172.16.255.20    1      1007     C,R       -

               1      1007     C,R       -
```

The following shows a sample output of OMP information on Cisco Catalyst SD-WAN Controllers:

```
Device# show omp l2-routes | tab

Code:
C   -> chosen
I   -> installed
Red -> redistributed
Rej -> rejected
L   -> looped
R   -> resolved
S   -> stale
Ext -> extranet
Inv -> invalid
Stg -> staged
IA  -> On-demand inactive
U   -> TLOC unresolved


                                                REMOTE
                                  ROUTE                     IP                    SITE
               PATH                   SITE
VPN    VC ID        ORIGINATOR       TYPE   MAC ADDRESS      ADDRESS  VPN TYPE    ID
FROM PEER        ID     LABEL    STATUS    ID
-------------------------------------------------------------------------------------------
12     12           172.16.255.15    vpn    0000.0000.0000   ::       p2p         500
172.16.255.15    66     1004     C,R       501

172.16.255.15    69     1004     C,R       501

172.16.255.20    1      1004     C,R       501

172.16.255.20    2      1004     C,R       501
12     12           172.16.255.27    vpn    0000.0000.0000   ::       p2p         501
172.16.255.20    1      1014     C,R       500

172.16.255.27    70     1014     C,R       500
13     13           172.16.255.15    vpn    0000.0000.0000   ::       multipoint  500
172.16.255.15    66     1006     C,R       -

172.16.255.15    69     1006     C,R       -

172.16.255.20    1      1006     C,R       -

172.16.255.20    2      1006     C,R       -
13     13           172.16.255.27    vpn    0000.0000.0000   ::       multipoint  501
172.16.255.20    1      1016     C,R       -

172.16.255.27    70     1016     C,R       -
13     13           172.16.255.32    vpn    0000.0000.0000   ::       multipoint  503
172.16.255.20    1      1007     C,R       -

172.16.255.32    71     1007     C,R       -
14     1            172.16.255.27    vpn    0000.0000.0000   ::       multipoint  501
172.16.255.20    1      1018     C,R       -
```

```
172.16.255.27    70     1018     C,R       -
15     1            172.16.255.15    vpn    0000.0000.0000   ::       p2p          500
172.16.255.15    66     1020     C,R       501

172.16.255.15    69     1020     C,R       501

172.16.255.20    1      1020     C,R       501

172.16.255.20    2      1020     C,R       501
15     1            172.16.255.27    vpn    0000.0000.0000   ::       p2p          501
172.16.255.20    1      1020     C,R       500

172.16.255.27    70     1020     C,R       500
```

```
Device# show omp l2-routes vpn 13 | tab

Code:
C   -> chosen
I   -> installed
Red -> redistributed
Rej -> rejected
L   -> looped
R   -> resolved
S   -> stale
Ext -> extranet
Inv -> invalid
Stg -> staged
IA  -> On-demand inactive
U   -> TLOC unresolved

                                                    REMOTE
                                      ROUTE                    IP                    SITE
                PATH                      SITE
VPN     VC ID         ORIGINATOR        TYPE   MAC ADDRESS      ADDRESS  VPN TYPE    ID
FROM PEER         ID     LABEL    STATUS    ID
-------------------------------------------------------------------------------------------
12      12            172.16.255.15    vpn    0000.0000.0000   ::       p2p          500
172.16.255.15    66     1004     C,R       501

172.16.255.15    69     1004     C,R       501

172.16.255.20    1      1004     C,R       501

172.16.255.20    2      1004     C,R       501
12      12            172.16.255.27    vpn    0000.0000.0000   ::       p2p          501
172.16.255.20    1      1014     C,R       500

172.16.255.27    70     1014     C,R       500
13      13            172.16.255.15    vpn    0000.0000.0000   ::       multipoint   500
172.16.255.15    66     1006     C,R       -

172.16.255.15    69     1006     C,R       -

172.16.255.20    1      1006     C,R       -

172.16.255.20    2      1006     C,R       -
13      13            172.16.255.27    vpn    0000.0000.0000   ::       multipoint   501
172.16.255.20    1      1016     C,R       -

172.16.255.27    70     1016     C,R       -
```

```
13     13           172.16.255.32    vpn    0000.0000.0000   ::       multipoint  503
172.16.255.20    1      1007     C,R       -

172.16.255.32    71     1007     C,R       -
14     1            172.16.255.27    vpn    0000.0000.0000   ::       multipoint  501
172.16.255.20    1      1018     C,R       -

172.16.255.27    70     1018     C,R       -
15     1            172.16.255.15    vpn    0000.0000.0000   ::       p2p         500
172.16.255.15    66     1020     C,R       501

172.16.255.15    69     1020     C,R       501

172.16.255.20    1      1020     C,R       501

172.16.255.20    2      1020     C,R       501
15     1            172.16.255.27    vpn    0000.0000.0000   ::       p2p         501
172.16.255.20    1      1020     C,R       500

172.16.255.27    70     1020     C,R       500
```

```
Device# show omp l2-routes vpn 13 vc-id 13 | tab

Code:
C   -> chosen
I   -> installed
Red -> redistributed
Rej -> rejected
L   -> looped
R   -> resolved
S   -> stale
Ext -> extranet
Inv -> invalid
Stg -> staged
IA  -> On-demand inactive
U   -> TLOC unresolved

                                                                REMOTE
                                      ROUTE                      IP                    SITE
                PATH                      SITE
VPN     VC ID         ORIGINATOR        TYPE    MAC ADDRESS      ADDRESS  VPN TYPE     ID
FROM PEER         ID      LABEL     STATUS     ID
-------------------------------------------------------------------------------------------
13     13           172.16.255.15    vpn    0000.0000.0000   ::       multipoint  500
172.16.255.15    66     1006     C,R       -

172.16.255.15    69     1006     C,R       -

172.16.255.20    1      1006     C,R       -

172.16.255.20    2      1006     C,R       -
13     13           172.16.255.27    vpn    0000.0000.0000   ::       multipoint  501
172.16.255.20    1      1016     C,R       -

172.16.255.27    70     1016     C,R       -
13     13           172.16.255.32    vpn    0000.0000.0000   ::       multipoint  503
172.16.255.20    1      1007     C,R       -

172.16.255.32    71     1007     C,R       -
```

show sdwan omp services

show sdwan omp services—Display the services learned from OMP peering sessions (on vSmart controllers and Cisco IOS XE Catalyst SD-WAN devices only).

Command Syntax

show sdwan omp services [**detail**]

Syntax Description

	None: List information about the services learned from OMP peering sessions.
detail	Detailed Information: Display detailed information.

Output Fields

The output fields are self-explanatory.

Command History

Release	Modification
16.12.1	Command introduced.

Usage Guidelines

The OMP services are not supported on IPv6 routes.

Example

```
vSmart# show sdwan omp services (command issued from a vSmart controller)
C   -> chosen
I   -> installed
Red -> redistributed
Rej -> rejected
L   -> looped
R   -> resolved
S   -> stale
Ext -> extranet
Inv -> invalid
                                                PATH
VPN  SERVICE  ORIGINATOR     FROM PEER      ID    LABEL  STATUS
-----------------------------------------------------------------------
1    VPN      172.16.255.11  172.16.255.11  3     32772  C,I,R
                             172.16.255.20  4     32772  R
1    VPN      172.16.255.14  172.16.255.14  3     18978  C,I,R
                             172.16.255.20  2     18978  R
1    VPN      172.16.255.15  172.16.255.15  3     19283  C,I,R
                             172.16.255.20  1     19283  R
1    VPN      172.16.255.16  172.16.255.16  3     3272   C,I,R
                             172.16.255.20  3     3272   R
1    VPN      172.16.255.21  172.16.255.20  5     53645  R
                             172.16.255.21  3     53645  C,I,R
```

show sdwan omp summary

Use the **show sdwan omp summary** to display information about the OMP sessions running between Cisco SD-WAN Controllers and Cisco IOS XE Catalyst SD-WAN devices (on Cisco SD-WAN Controllers and Cisco IOS XE Catalyst SD-WAN devices only).

Command Syntax

show sdwan omp summary [*parameter-name*]

Syntax Description

	None: List information about the OMP peering sessions running on the local device
parameter-name	Information about a Specific Parameter: Display configuration information about a specific OMP peering session parameter. *parameter-name* can be one of the following: **adminstate**, **devicetype**, **ompdowntime**, **ompuptime**, **operstate**, **peers**, **routes-installed**, **routes-received**, **routes-sent**, **services-installed**, **services-sent**, **tlocs-installed**, **tlocs-received**, **tlocs-sent**, and **vsmart-peers**. For an explanation of these parameters, see the Output Fields below.

Output Fields

Field	Explanation
admin-state	Administrative state of the OMP session. It can be UP or DOWN.
omp-uptime	How long the OMP session has been up and operational.
oper-state	Operational status of the OMP session. It can be UP or DOWN.
personality	Cisco IOS XE Catalyst SD-WAN device personality.
region-id	Region ID, for the Multi-Region Fabric feature.
routes-installed	Number of routes installed over the OMP session.
routes-received	Number of routes received over the OMP session.
routes-sent	Number of routes sent over the OMP session.
services-installed	Number of services installed that were learned over OMP sessions.
services-received	Number of services received over OMP sessions.
services-sent	Number of services advertised over OMP sessions.

Field	Explanation
sub-region-id	Subregion ID, for the Multi-Region Fabric feature.
tlocs-installed	Number of TLOCs installed that were learned over OMP sessions.
tlocs-received	Number of TLOCs received over OMP sessions.
tlocs-sent	Number of TLOCs advertised over OMP sessions.
transport-gateway	Indicates the enabled/disabled status of the transport gateway feature.
vsmart-peers	Number of vSmart peers that are up.

Command History

Release	Modification
16.12.1	Command introduced.
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	Added **transport-gateway** to the output to indicate the enabled/disabled status.
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	Added Multi-Region Fabric subregion information to the output. For information about subregions, see the Cisco SD-WAN Multi-Region Fabric (also Hierarchical SD-WAN) Configuration Guide.

Example

The following sample output includes the **region-id** and **sub-region-id** of a device. These fields are relevant for a device operating in a network using Multi-Region Fabric.

```
Device#show sdwan omp summary
oper-state              UP
admin-state             UP
personality             vedge
device-role             Edge-Router
omp-uptime              0:00:56:17
routes-received         194
routes-installed        58
routes-sent             12
tlocs-received          25
tlocs-installed         11
tlocs-sent              6
services-received       3
services-installed      0
services-sent           6
mcast-routes-received   0
mcast-routes-installed  0
mcast-routes-sent       0
hello-sent              1351
hello-received          1344
handshake-sent          2
```

```
handshake-received     2
alert-sent             0
alert-received         0
inform-sent            26
inform-received        26
update-sent            30
update-received        254
policy-sent            0
policy-received        0
total-packets-sent     1409
total-packets-received 1628
vsmart-peers           2
region-id              1
sub-region-id          5
secondary-region-id    None
```

```
Device# show sdwan omp summary
oper-state             UP
admin-state            UP
personality            vedge
omp-uptime             0:19:05:45
routes-received        16
routes-installed       8
routes-sent            0
tlocs-received         7
tlocs-installed        3
tlocs-sent             2
services-received      1
services-installed     0
services-sent          2
mcast-routes-received  0
mcast-routes-installed 0
mcast-routes-sent      0
hello-sent             27471
hello-received         27460
hsndshake-sent         6
handshake-received     6
alert-sent             2
alert-received         2
inform-sent            8
inform-received        8
update-sent            48
update-received        213
policy-sent            0
policy-received        0
total-packets-sent     27535
total-packets-received 27689
vsmart-peers           2
```

```
vSmart# show sdwan omp summary
oper-state             UP
admin-state            UP
personality            vsmart
omp-uptime             0:19:07:20
routes-received        18
routes-installed       0
routes-sent            32
tlocs-received         8
tlocs-installed        4
tlocs-sent             16
services-received      8
services-installed     4
services-sent          4
```

```
mcast-routes-received  0
mcast-routes-installed 0
mcast-routes-sent      0
hello-sent             80765
hello-received         80782
hsndshake-sent         13
handshake-received     13
alert-sent             4
alert-received         4
inform-sent            24
inform-received        24
update-sent            633
update-received        278
policy-sent            0
policy-received        0
total-packets-sent     81439
total-packets-received 81101
vsmart-peers           1
vedge-peers            4
```

show sdwan omp tlocs

Use the **show sdwan omp tlocs** to display information learned from the TLOC routes advertised over the OMP sessions running between Cisco SD-WAN Controllers and Cisco IOS XE Catalyst SD-WAN devices (on Cisco SD-WAN Controllers and Cisco IOS XE Catalyst SD-WAN devices only).

Command Syntax

show sdwan omp tlocs [**detail**]

Syntax Description

	None: List information about all TLOCs that the local device has learned about.
detail	Detailed Information: Show detailed information.

Output Fields

The output fields are self-explanatory.

Command History

Release	Modification
16.12	Command introduced.
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	Added Multi-Region Fabric subregion information to the output. For information about subregions, see the Cisco SD-WAN Multi-Region Fabric (also Hierarchical SD-WAN) Configuration Guide.

Example

In the following sample output, the **Region ID** column indicates either **1** for region 1, or **1.5** for subregion 5 of region 1.

```
Device#show sdwan omp tlocs table
```

```
                                        PUBLIC           PRIVATE                    AFFINITY
ADDRESS                                 TENANT                          PSEUDO                    PUBLIC
                     PRIVATE  PUBLIC    IPV6    PRIVATE  IPV6     BFD                GROUP
FAMILY   TLOC IP      COLOR  ENCAP     ID       FROM PEER        STATUS    KEY     PUBLIC IP        PORT
   PRIVATE IP         PORT    IPV6      PORT    IPV6     PORT    STATUS  REGION ID   NUMBER
-------------------------------------------------------------------------------------------------------
ipv4     175.1.11.10  lte     ipsec     0        175.0.122.10     C,I,R     1       172.1.11.11      12366
   172.1.11.11       12366   ::        0       ::       0        up      1.5         None
                                        0        175.0.123.10     C,R       1       172.1.11.11      12366
   172.1.11.11       12366   ::        0       ::       0        up      1.5         None
         175.1.11.10  3g      ipsec     0        175.0.122.10     C,I,R     1       173.1.11.11      12366
   173.1.11.11       12366   ::        0       ::       0        up      1.5         None
                                        0        175.0.123.10     C,R       1       173.1.11.11      12366
   173.1.11.11       12366   ::        0       ::       0        up      1.5         None
         175.1.11.10  red     ipsec     0        175.0.122.10     C,I,R     1       172.1.12.11      5062
   173.174.11.1      12366   ::        0       ::       0        up      1.5         None
                                        0        175.0.123.10     C,R       1       172.1.12.11      5062
   173.174.11.1      12366   ::        0       ::       0        up      1.5         None
         175.1.12.10  lte     ipsec     0        175.0.122.10     C,I,R     1       172.1.12.11      12366
   172.1.12.11       12366   ::        0       ::       0        up      1           None
                                        0        175.0.123.10     C,R       1       172.1.12.11      12366
   172.1.12.11       12366   ::        0       ::       0        up      1           None
         175.1.12.10  3g      ipsec     0        175.0.122.10     C,I,R     1       173.1.12.11      12366
   173.1.12.11       12366   ::        0       ::       0        up      1           None
                                        0        175.0.123.10     C,R       1       173.1.12.11      12366
   173.1.12.11       12366   ::        0       ::       0        up      1           None
         175.1.12.10  red     ipsec     0        175.0.122.10     C,I,R     1       172.1.11.11      5062
   173.174.12.1      12366   ::        0       ::       0        up      1           None
                                        0        175.0.123.10     C,R       1       172.1.11.11      5062
   173.174.12.1      12366   ::        0       ::       0        up      1           None
         175.1.51.10  lte     ipsec     0        0.0.0.0          C,Red,R   1       172.1.1.11       12366
   172.1.1.11        12366   ::        0       ::       0        up      1.5         None
         175.1.51.10  3g      ipsec     0        0.0.0.0          C,Red,R   1       173.1.1.11       12366
   173.1.1.11        12366   ::        0       ::       0        up      1.5         None
         175.1.51.10  red     ipsec     0        0.0.0.0          C,Red,R   1       172.1.2.11       5062
   173.174.1.1       12366   ::        0       ::       0        up      1.5         None
         175.1.52.10  lte     ipsec     0        175.0.122.10     C,I,R     1       172.1.2.11       12366
   172.1.2.11        12366   ::        0       ::       0        up      1.5         None
                                        0        175.0.123.10     C,R       1       172.1.2.11       12366
   172.1.2.11        12366   ::        0       ::       0        up      1.5         None
```

```
Device# show sdwan omp tlocs
Code:
C   -> chosen
I   -> installed
Red -> redistributed
Rej -> rejected
L   -> looped
R   -> resolved
S   -> stale
Ext -> extranet
Inv -> invalid
```

```
          PUBLIC           PRIVATE                                                  PSEUDO                  PUBLIC                  PRIVATE
  PUBLIC  IPV6    PRIVATE  IPV6     BFD
TLOC IP           COLOR            ENCAP  FROM PEER        STATUS    KEY     PUBLIC IP        PORT    PRIVATE IP       PORT
  IPV6    PORT    IPV6     PORT     STATUS
-------------------------------------------------------------------------------------------------------------------------------
172.16.254.1     lte              ipsec  172.16.254.1     C,I,R     1       10.102.2.2       12366   10.102.2.2       12366
  ::      0       ::       0        -
                                         172.16.255.132   C,R       1       10.102.2.2       12366   10.102.2.2       12366
  ::      0       ::       0        -
172.16.254.1     3g               ipsec  172.16.254.1     C,I,R     1       10.101.2.2       12366   10.101.2.2       12366
```

```
  ::      0       ::       0        -
                                     172.16.255.132   C,R       1       10.101.2.2       12366   10.101.2.2       12366
  ::      0       ::       0        -
172.16.254.2     lte              ipsec  172.16.254.2     C,I,R     1       10.102.3.3       12366   10.102.3.3       12366
  ::      0       ::       0        -
                                     172.16.255.132   C,R       1       10.102.3.3       12366   10.102.3.3       12366
  ::      0       ::       0        -
172.16.254.2     3g               ipsec  172.16.254.2     C,I,R     1       10.101.3.3       12366   10.101.3.3       12366
  ::      0       ::       0        -
                                     172.16.255.132   C,R       1       10.101.3.3       12366   10.101.3.3       12366
  ::      0       ::       0        -
172.16.254.3     lte              ipsec  172.16.254.3     C,I,R     1       10.102.4.4       12366   10.102.4.4       12366
  ::      0       ::       0        -
                                     172.16.255.132   C,R       1       10.102.4.4       12366   10.102.4.4       12366
  ::      0       ::       0        -
172.16.254.3     3g               ipsec  172.16.254.3     C,I,R     1       10.101.4.4       12366   10.101.4.4       12366
  ::      0       ::       0        -
                                     172.16.255.132   C,R       1       10.101.4.4       12366   10.101.4.4       12366
  ::      0       ::       0        -
172.16.254.4     lte              ipsec  172.16.254.4     C,I,R     1       10.102.5.5       12366   10.102.5.5       12366
  ::      0       ::       0        -
                                     172.16.255.132   C,R       1       10.102.5.5       12366   10.102.5.5       12366
  ::      0       ::       0        -
172.16.254.4     3g               ipsec  172.16.254.4     C,I,R     1       10.101.5.5       12366   10.101.5.5       12366
  ::      0       ::       0        -
                                     172.16.255.132   C,R       1       10.101.5.5       12366   10.101.5.5       12366
  ::      0       ::       0        -
172.16.254.5     lte              ipsec  172.16.254.5     C,I,R     1       10.102.6.6       12366   10.102.6.6       12366
  ::      0       ::       0        -
                                     172.16.255.132   C,R       1       10.102.6.6       12366   10.102.6.6       12366
  ::      0       ::       0        -
172.16.254.5     3g               ipsec  172.16.254.5     C,I,R     1       10.101.6.6       12366   10.101.6.6       12366
  ::      0       ::       0        -
                                     172.16.255.132   C,R       1       10.101.6.6       12366   10.101.6.6       12366
  ::      0       ::       0        -

vEdge# show sdwan omp tlocs advertised
Code:
C   -> chosen
I   -> installed
Red -> redistributed
Rej -> rejected
L   -> looped
R   -> resolved
S   -> stale
Ext -> extranet
Inv -> invalid

          PUBLIC           PRIVATE
                                                                                PSEUDO                  PUBLIC                  PRIVATE
  PUBLIC  IPV6    PRIVATE  IPV6     BFD
TLOC IP           COLOR            ENCAP  FROM PEER        STATUS    KEY     PUBLIC IP        PORT    PRIVATE IP       PORT
  IPV6    PORT    IPV6     PORT     STATUS
--------------------------------------------------------------------------------------------------------------------------------------
172.16.254.1     lte              ipsec  172.16.254.1     C,I,R     1       10.102.2.2       12366   10.102.2.2       12366
  ::      0       ::       0        -
                                     172.16.255.132   C,R       1       10.102.2.2       12366   10.102.2.2       12366
  ::      0       ::       0        -
172.16.254.1     3g               ipsec  172.16.254.1     C,I,R     1       10.101.2.2       12366   10.101.2.2       12366
  ::      0       ::       0        -
                                     172.16.255.132   C,R       1       10.101.2.2       12366   10.101.2.2       12366
  ::      0       ::       0        -
172.16.254.2     lte              ipsec  172.16.254.2     C,I,R     1       10.102.3.3       12366   10.102.3.3       12366
  ::      0       ::       0        -
                                     172.16.255.132   C,R       1       10.102.3.3       12366   10.102.3.3       12366
  ::      0       ::       0        -
172.16.254.2     3g               ipsec  172.16.254.2     C,I,R     1       10.101.3.3       12366   10.101.3.3       12366
  ::      0       ::       0        -
                                     172.16.255.132   C,R       1       10.101.3.3       12366   10.101.3.3       12366
  ::      0       ::       0        -
172.16.254.3     lte              ipsec  172.16.254.3     C,I,R     1       10.102.4.4       12366   10.102.4.4       12366
  ::      0       ::       0        -
                                     172.16.255.132   C,R       1       10.102.4.4       12366   10.102.4.4       12366
```

```
  ::      0       ::       0        -
172.16.254.3     3g              ipsec  172.16.254.3     C,I,R     1       10.101.4.4       12366   10.101.4.4       12366
  ::      0       ::       0        -
                                        172.16.255.132   C,R       1       10.101.4.4       12366   10.101.4.4       12366
  ::      0       ::       0        -
172.16.254.4     lte             ipsec  172.16.254.4     C,I,R     1       10.102.5.5       12366   10.102.5.5       12366
  ::      0       ::       0        -
                                        172.16.255.132   C,R       1       10.102.5.5       12366   10.102.5.5       12366
  ::      0       ::       0        -
172.16.254.4     3g              ipsec  172.16.254.4     C,I,R     1       10.101.5.5       12366   10.101.5.5       12366
  ::      0       ::       0        -
                                        172.16.255.132   C,R       1       10.101.5.5       12366   10.101.5.5       12366
  ::      0       ::       0        -
172.16.254.5     lte             ipsec  172.16.254.5     C,I,R     1       10.102.6.6       12366   10.102.6.6       12366
  ::      0       ::       0        -
                                        172.16.255.132   C,R       1       10.102.6.6       12366   10.102.6.6       12366
  ::      0       ::       0        -
172.16.254.5     3g              ipsec  172.16.254.5     C,I,R     1       10.101.6.6       12366   10.101.6.6       12366
  ::      0       ::       0        -
                                        172.16.255.132   C,R       1       10.101.6.6       12366   10.101.6.6       12366
  ::      0       ::       0        -
```

```
vEdge# show sdwan omp tlocs received
Code:
C   -> chosen
I   -> installed
Red -> redistributed
Rej -> rejected
L   -> looped
R   -> resolved
S   -> stale
Ext -> extranet
Inv -> invalid
```

```
          PUBLIC           PRIVATE                                                                PSEUDO                  PUBLIC                  PRIVATE
  PUBLIC  IPV6    PRIVATE  IPV6     BFD
TLOC IP           COLOR            ENCAP  FROM PEER        STATUS    KEY     PUBLIC IP        PORT    PRIVATE IP       PORT
  IPV6    PORT    IPV6     PORT     STATUS
-------------------------------------------------------------------------------------------------------------------------------------------------------
172.16.254.1     lte             ipsec  172.16.254.1     C,I,R     1       10.102.2.2       12366   10.102.2.2       12366
  ::      0       ::       0        -
                                        172.16.255.132   C,R       1       10.102.2.2       12366   10.102.2.2       12366
  ::      0       ::       0        -
172.16.254.1     3g              ipsec  172.16.254.1     C,I,R     1       10.101.2.2       12366   10.101.2.2       12366
  ::      0       ::       0        -
                                        172.16.255.132   C,R       1       10.101.2.2       12366   10.101.2.2       12366
  ::      0       ::       0        -
172.16.254.2     lte             ipsec  172.16.254.2     C,I,R     1       10.102.3.3       12366   10.102.3.3       12366
  ::      0       ::       0        -
                                        172.16.255.132   C,R       1       10.102.3.3       12366   10.102.3.3       12366
  ::      0       ::       0        -
172.16.254.2     3g              ipsec  172.16.254.2     C,I,R     1       10.101.3.3       12366   10.101.3.3       12366
  ::      0       ::       0        -
                                        172.16.255.132   C,R       1       10.101.3.3       12366   10.101.3.3       12366
  ::      0       ::       0        -
172.16.254.3     lte             ipsec  172.16.254.3     C,I,R     1       10.102.4.4       12366   10.102.4.4       12366
  ::      0       ::       0        -
                                        172.16.255.132   C,R       1       10.102.4.4       12366   10.102.4.4       12366
  ::      0       ::       0        -
172.16.254.3     3g              ipsec  172.16.254.3     C,I,R     1       10.101.4.4       12366   10.101.4.4       12366
  ::      0       ::       0        -
                                        172.16.255.132   C,R       1       10.101.4.4       12366   10.101.4.4       12366
  ::      0       ::       0        -
172.16.254.4     lte             ipsec  172.16.254.4     C,I,R     1       10.102.5.5       12366   10.102.5.5       12366
  ::      0       ::       0        -
                                        172.16.255.132   C,R       1       10.102.5.5       12366   10.102.5.5       12366
  ::      0       ::       0        -
172.16.254.4     3g              ipsec  172.16.254.4     C,I,R     1       10.101.5.5       12366   10.101.5.5       12366
  ::      0       ::       0        -
                                        172.16.255.132   C,R       1       10.101.5.5       12366   10.101.5.5       12366
  ::      0       ::       0        -
172.16.254.5     lte             ipsec  172.16.254.5     C,I,R     1       10.102.6.6       12366   10.102.6.6       12366
```

```
  ::      0       ::       0        -
                                        172.16.255.132   C,R       1       10.102.6.6       12366   10.102.6.6       12366
  ::      0       ::       0        -
172.16.254.5     3g               ipsec  172.16.254.5     C,I,R     1       10.101.6.6       12366   10.101.6.6       12366
  ::      0       ::       0        -
                                        172.16.255.132   C,R       1       10.101.6.6       12366   10.101.6.6       12366
  ::      0       ::       0        -
vEdge# show sdwan omp tlocs detail

--------------------------------------------------
tloc entries for 172.16.254.1
                lte
                ipsec
--------------------------------------------------
           RECEIVED FROM:
peer            172.16.254.1
status          C,I,R
loss-reason     not set
lost-to-peer    not set
lost-to-path-id not set
    Attributes:
     attribute-type    installed
     encap-key         not set
     encap-proto       0
     encap-spi         376
     encap-auth        sha1-hmac,ah-sha1-hmac
     encap-encrypt     aes256
     public-ip         10.102.2.2
     public-port       12366
     private-ip        10.102.2.2
     private-port      12366
     public-ip         ::
     public-port       0
     private-ip        ::
     private-port      0
     domain-id         not set
     site-id           2
     overlay-id        not set
     preference        0
     tag               not set
     stale             not set
     weight            1
     version           2
    gen-id             0x80000000
     carrier           default
     restrict          0
     groups            [ 0 ]
     border             not set
     unknown-attr-len  not set
           RECEIVED FROM:
peer            172.16.255.132
status          C,R
loss-reason     not set
lost-to-peer    not set
lost-to-path-id not set
    Attributes:
     attribute-type    installed
     encap-key         not set
     encap-proto       0
     encap-spi         376
     encap-auth        sha1-hmac,ah-sha1-hmac
     encap-encrypt     aes256
     public-ip         10.102.2.2
     public-port       12366
     private-ip        10.102.2.2
     private-port      12366
     public-ip         ::
     public-port       0
     private-ip        ::
     private-port      0
     domain-id         not set
     site-id           2
     overlay-id        not set
```

```
     preference        0
     tag               not set
     stale             not set
     weight            1
     version           2
    gen-id             0x80000000
     carrier           default
     restrict          0
     groups            [ 0 ]
     border             not set
     unknown-attr-len  not set
           ADVERTISED TO:
peer    172.16.254.2
    Attributes:
     encap-key         not set
     encap-proto       0
     encap-spi         376
     encap-auth        sha1-hmac,ah-sha1-hmac
     encap-encrypt     des,des3
     public-ip         10.102.2.2
     public-port       12366
     private-ip        10.102.2.2
     private-port      12366
     public-ip       ::
     public-port     0
     private-ip      ::
     private-port     0
     domain-id         not set
     site-id           2
     overlay-id        not set
     preference        0
     tag               not set
     stale             not set
     weight            1
     version           2
     gen-id            0x80000000
     carrier           default
     restrict          0
     groups            [ 0 ]
     border              not set
     unknown-attr-len  not set
           ADVERTISED TO:
peer    172.16.254.3
    Attributes:
     encap-key         not set
     encap-proto       0
     encap-spi         376
     encap-auth        sha1-hmac,ah-sha1-hmac
     encap-encrypt     des,des3
     public-ip         10.102.2.2
     public-port       12366
     private-ip        10.102.2.2
     private-port      12366
     public-ip       ::
     public-port     0
     private-ip      ::
     private-port     0
     domain-id         not set
     site-id           2
     overlay-id        not set
     preference        0
     tag               not set
     stale             not set
     weight            1
     version           2
     gen-id            0x80000000
     carrier           default
     restrict          0
     groups            [ 0 ]
     border              not set
     unknown-attr-len  not set
           ADVERTISED TO:
peer    172.16.254.4
```

```
    Attributes:
     encap-key         not set
     encap-proto       0
     encap-spi         376
     encap-auth        sha1-hmac,ah-sha1-hmac
     encap-encrypt     des,des3
     public-ip         10.102.2.2
     public-port       12366
     private-ip        10.102.2.2
     private-port      12366
     public-ip       ::
     public-port     0
     private-ip      ::
     private-port     0
     domain-id         not set
     site-id           2
     overlay-id        not set
     preference        0
     tag               not set
     stale             not set
     weight            1
     version           2
     gen-id            0x80000000
     carrier           default
     restrict          0
     groups            [ 0 ]
     border              not set
     unknown-attr-len  not set
           ADVERTISED TO:
peer    172.16.254.5
    Attributes:
     encap-key         not set
     encap-proto       0
     encap-spi         376
     encap-auth        sha1-hmac,ah-sha1-hmac
     encap-encrypt     des,des3
     public-ip         10.102.2.2
     public-port       12366
     private-ip        10.102.2.2
     private-port      12366
     public-ip       ::
     public-port     0
     private-ip      ::
     private-port     0
     domain-id         not set
     site-id           2
     overlay-id        not set
     preference        0
     tag               not set
     stale             not set
     weight            1
     version           2
     gen-id            0x80000000
     carrier           default
     restrict          0
     groups            [ 0 ]
     border              not set
     unknown-attr-len  not set
           ADVERTISED TO:
peer    172.16.255.132
    Attributes:
     encap-key         not set
     encap-proto       0
     encap-spi         376
     encap-auth        sha1-hmac,ah-sha1-hmac
     encap-encrypt     des,des3
     public-ip         10.102.2.2
     public-port       12366
     private-ip        10.102.2.2
     private-port      12366
     public-ip       ::
     public-port     0
     private-ip      ::
```

```
    private-port     0
    domain-id         not set
    site-id           2
    overlay-id        not set
    preference        0
    tag               not set
    stale             not set
    weight            1
    version           2
    gen-id            0x80000000
    carrier           default
    restrict          0
    groups            [ 0 ]
    border              not set
    unknown-attr-len  not set
...
```

show sdwan policy access-list-associations

Display the IPv4 access lists that are operating on each interface.

show sdwan policy access-list-associations [*access-list-name*]

Syntax Description

None	Display all access lists operating on the router's interfaces.
Specific Access List	*access-list-name* Display the interfaces on which the specific access list is operating.

Examples

Show sdwan policy access-list-associations

```
Device# show running-config policy
policy
 access-list ALLOW_OSPF_PACKETS
  sequence 65535
   match
    protocol 89
   !
   action accept
    count count_OSPF_PACKETS
   !
  !
  default-action accept
 !
!

Device# show policy access-list-associations

                    INTERFACE  INTERFACE
NAME                NAME       DIRECTION
------------------------------------------
ALLOW_OSPF_PACKETS  ge0/0      in
```

show sdwan policy access-list-counters

Display the IPv4 access lists that are operating on each interface.

show sdwan policy access-list-counters [*access-list-name*]

Syntax Description

None	Display all access lists operating on the router's interfaces.
Specific Access List	*access-list-name* Display the interfaces on which the specific access list is operating.

Examples

Show sdwan policy access-list-counters

```
Device# show running-config policy
policy
 access-list ALLOW_OSPF_PACKETS
  sequence 65535
   match
    protocol 89
   !
   action accept
    count count_OSPF_PACKETS
   !
  !
  default-action accept
 !
!

Device# show policy access-list-associations

                   INTERFACE  INTERFACE
NAME               NAME       DIRECTION
-----------------------------------------
ALLOW_OSPF_PACKETS  ge0/0      in
```

show sdwan policy data-policy-filter

show sdwan policy access-list-names

Display the names of the IPv4 access lists configured on the devices.

show sdwan policy access-list-names

Syntax Description

Syntax Description None

Examples

Show sdwan policy access-list-names

```
Device# show running-config policy
policy
 access-list ALLOW_OSPF_PACKETS
  sequence 65535
   match
    protocol 89
   !
   action accept
    count count_OSPF_PACKETS
   !
  !
  default-action accept
 !
!
Device# show policy access-list-names

NAME
--------------------
ALLOW_OSPF_PACKETS
```

show sdwan policy access-list-policers

Display information about the policers configured in IPv4 access lists.

show sdwan policy access-list-policers

Syntax Description

None

Example

Display a list of policers configured in access lists. This output shows that the policer named "p1_police" was applied in sequence 10 in the access list "acl_p1" in sequences 10, 20, and 30 in the "acl_plp" access list.

```
Device# show sdwan policy access-list-policers
                                    OOS
NAME                POLICER NAME    PACKETS
-------------------------------------------
acl_p1              10.p1_police    0
acl_plp             10.p1_police    0
                    20.p1_police    0
                    30.p2_police    0
```

show sdwan policy app-route-policy-filter

To display information about application-aware routing policy matched packet counts on Cisco IOS XE SD-WAN devices, use the **show sdwan policy app-route-policy-filter** command in privileged EXEC mode.

show sdwan policy app-route-policy-filter [*policy-name*]

Syntax Description

policy-name	(Optional) Displays information about the application-aware routing policy matched packet counts for the specified policy.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Application-aware routing tracks network and path characteristics of the data plane tunnels between Cisco IOS XE SD-WAN devices, and uses the collected information to compute optimal paths for data traffic.

An application-aware routing policy matches applications with an SLA, that is, with the data plane tunnel performance characteristics that are necessary to transmit the applications' data traffic. When a data packet matches one of the match conditions, an SLA action is applied to the packet to determine the data plane tunnel to transmit the packet.

This command can be used to display information about application-aware routing policy matched packet counts on Cisco IOS XE SD-WAN devices.

Example

The following example shows how to display information about application-aware routing policy matched packet counts on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan policy app-route-policy-filter
NAME                NAME     COUNTER NAME           PACKETS       BYTES
----------------------------------------------------------------------
_ALLVPNs_Test-AAR   ALLVPNs  default_action_count   12            2936
```

The following example shows how to display information about application-aware routing policy matched packet counts for the specified policy on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan policy app-route-policy-filter _ALLVPNs_Test-AAR
NAME                NAME     COUNTER NAME           PACKETS       BYTES
----------------------------------------------------------------------
_ALLVPNs_Test-AAR   ALLVPNs  default_action_count   12            2936
```

Related Commands

Command	Description
show sdwan ipsec inbound-connections	Displays SD-WAN policy access-list-associations.
show sdwan ipsec inbound-connections	Displays SD-WAN policy access-list-counters.
show sdwan ipsec inbound-connections	Displays SD-WAN policy access-list-names.
show sdwan ipsec inbound-connections	Displays SD-WAN policy access-list-policers.

Command	Description
show sdwan ipsec inbound-connections	Displays SD-WAN policy data-policy-filter.
show sdwan policy from-vsmart	Displays SD-WAN policy from Cisco Catalyst SD-WAN Controller.
show sdwan policy ipv6	Displays SD-WAN policy IPv6.
show sdwan policy rewrite-associations	Displays SD-WAN policy rewrite-associations.
show sdwan policy service-path	Displays next-hop information for packet coming from service side.
show sdwan policy tunnel-path	Displays next-hop information for packet coming over the WAN tunnel.

show sdwan policy data-policy-filter

Display information about data policy filters for configured counters.

show sdwan policy data-policy-filter

Syntax Description

None

Examples

Example 1

Display the number of packets and bytes for four configured data policy counters:

```
vSmart# show running-config policy data-policy
policy
 data-policy Local-City-Branch
   vpn-list-Guest-VPN
    sequence 10
      action accetp
        count Guest-Wifi-Traffic
        cflod
      !
    !
    default-action accept
  !
  vpn-list Service-VPN
    sequence 10
      match
        destination-data-prefix-list Business-Prefixes
        destination-port 80
      !
      action accept
        count Business-Traffic
        cflowd
      !
    !
    sequence 20
      match
```

```
        destination-port 10090
        protocol 6
      !
      action accept
        count Other-Branch-Traffic
        cflowd
      !
    !
    sequence 30
      action accept
        count Misc-Traffic
        cflowd
      !
    !
    default-action accept
  !
!

vEdge# show policy data-policy-filter
                                                                                    POLICER    OOS      OOS
NAME                    NAME         COUNTER NAME          PACKETS     BYTES        NAME       PACKETS  BYTES
-------------------------------------------------------------------------------------------------------------
Local-City-Branch       Guest-VPN    Guest-Wifi-Traffic    18066728    12422330320
                        Service-VPN  Business-Traffic      92436       7082643
                                     Other-Branch-Traffic  1663339139  163093277861
                                     Misc-Traffic          32079661    5118593007
```

Example 3

For a data policy that includes a policer, display the policers:

```
Device# show policy from-vsmart
from-vsmart data-policy dp1
 direction from-service
 vpn-list vpn_1_list
  sequence 10
   match
    protocol 1
   action accept
    count police_count
    set
     policer police
  sequence 20
   action accept
    count police_count20
    set
     policer police
  sequence 30
   action accept
    set
     policer police
  default-action accept
from-vsmart policer police
 rate   10000000
 burst  1000000
 exceed remark
from-vsmart lists vpn-list vpn_1_list
 vpn 1

Device# show sdwan policy data-policy-filter

                                                 POLICER    OOS      OOS
NAME  NAME         COUNTER NAME    PACKETS  BYTES  NAME       PACKETS  BYTES
------------------------------------------------------------------------------
dp1   vpn_1_list  police_count    0        0
```

```
police_count20  0        0      10.police  0
                                20.police  0
                                30.police  0
```

show sdwan policy from-vsmart

To display a centralized data policy, an application-aware policy, or a cflowd policy that a Cisco SD-WAN Controller has pushed to the devices, use the **show sdwan policy from-vsmart** command in privileged EXEC mode. The Cisco SD-WAN Controller pushes the policy via OMP after it has been configured and activated on the controller.

show sdwan policy from-vsmart [**app-route-policy**] [**cflowd-template** *template-option*] [**data-policy**] [**lists** { **data-prefix-list** | **vpn-list** }] [**policer**] [**sla-class**]

Syntax Description

None	Display all the data policies that the vSmart controller has pushed to the Cisco IOS XE Catalyst SD-WAN device.
app-route-policy	Display only the application-aware routing policies that the Cisco vSmart controller has pushed to the Cisco IOS XE Catalyst SD-WAN device.
cflowd-template [*template-option*]	Display only the cflowd template information that the Cisco vSmart controller has pushed to the Cisco IOS XE Catalyst SD-WAN device. *template-option* can be one of **collector**, **flow-active-timeout**, **flow-inactive-timeout**, and **template-refresh**.
data-policy	Display only the data policies that the Cisco vSmart controller has pushed to the Cisco IOS XE Catalyst SD-WAN device.
lists {**data-prefix-list** | **vpn-list**}	Display only the policy-related lists that the Cisco vSmart controller has pushed to the Cisco IOS XE Catalyst SD-WAN device.
policer	Display only the policers that the Cisco vSmart controller has pushed to the Cisco IOS XE Catalyst SD-WAN device.
sla-class	Display only the SLA classes for application-aware routing that the Cisco vSmart controller has pushed to the Cisco IOS XE Catalyst SD-WAN device.

Examples

The following is a sample output from the **show sdwan policy from-vsmart** command displaying policy downloaded from Cisco SD-WAN Controller:

```
Device# show sdwan policy from-vsmart
from-vsmart sla-class SLA1
 latency 100
from-vsmart data-policy DATA_POLICY
 direction from-service
 vpn-list vpn_1
  sequence 11
   match
    destination-port         5060
    protocol                 17
    source-tag-instance      DP_V4_TAG1
    destination-tag-instance DP_V4_TAG3
```

```
   action accept
    count src_dst_legacy_v4
  sequence 21
   match
    source-tag-instance DP_V4_TAG1
   action drop
    count src_v4


Device# show sdwan policy from-vsmart
from-vsmart sla-class test_sla_class
 latency 50
from-vsmart app-route-policy test_app_route_policy
 vpn-list vpn_1_list
  sequence 1
   match
    destination-ip 10.2.3.21/32
   action
    sla-class test_sla_class
    sla-class strict
  sequence 2
   match
    destination-port 80
   action
    sla-class test_sla_class
    no sla-class strict
  sequence 3
   match
    destination-data-prefix-list test_data_prefix_list
   action
    sla-class test_sla_class
    sla-class strict

from-vsmart lists vpn-list vpn_1_list
 vpn 1
 vpn 102
from-vsmart lists data-prefix-list test_data_prefix_list
 ip-prefix 10.60.1.0/24


Device# show sdwan policy from-vsmart cflowd-template
from-vsmart cflowd-template test-cflowd-template
 flow-active-timeout   30
 flow-inactive-timeout 30
 template-refresh      30
 collector vpn 1 address 172.16.255.15 port 13322
Device# show policy from-vsmart cflowd-template collector
from-vsmart cflowd-template test-cflowd-template
 collector vpn 1 address 172.16.255.15 port 13322
```

show sdwan policy ipv6 access-list-associations

show sdwan policy ipv6 access-list-associations—Display the IPv6 access lists that are operating on each interface.

Command Syntax

show sdwan policy ipv6 access-list-associations

Syntax Description

None

Output Fields

The output fields are self-explanatory.

Command History

Release	Modification
16.3	Command introduced.

Example

```
Device# show sdwan policy ipv6 access-list-associations

            INTERFACE  INTERFACE
NAME        NAME       DIRECTION
------------------------------------------
ipv6-policy  ge0/2     out
```

show sdwan policy ipv6 access-list-counters

show sdwan policy ipv6 access-list-counters—Display the number of packets counted by IPv6 access lists configured on the Cisco IOS XE Catalyst SD-WAN device.

Command Syntax

show sdwan policy ipv6 access-list-counters

Syntax Description

None

Output Fields

The output fields are self-explanatory.

Command History

Release	Modification
16.3	Command introduced.

Example

```
Device# show sdwan policy ipv6 access-list-counters

NAME         COUNTER NAME  PACKETS  BYTES
```

```
-----------------------------------------------------------
ipv6-policy  ipv6-counter  1634     135940
```

show sdwan policy ipv6 access-list-names

show sdwan policy ipv6 access-list-names—Display the names of the IPv6 access lists configured on the Cisco IOS XE Catalyst SD-WAN device.

Command Syntax

show sdwan policy ipv6 access-list-names

Syntax Description

None

Output Fields

The output fields are self-explanatory.

Command History

Release	Modification
16.3	Command introduced.

Examples

```
Device# show sdwan policy ipv6 access-list-names

NAME
--------------------
ipv6-policy
```

show sdwan policy ipv6 access-list-policers

show sdwan policy ipv6 access-list-policers—Display information about the policers configured in IPv6 access lists.

Command Syntax

show sdwan policy ipv6 access-list-policers

Syntax Description

None

Output Fields

The output fields are self-explanatory.

Command History

Release	Modification
16.3	Command introduced.

Examples

Display a list of policers configured in access lists. This output shows that the policer named "p1_police" was applied in sequence 10 in the access list "ipv6_p1" in sequences 10, 20, and 30 in the "ipv6_plp" access list.

```
Device# show sdwan policy ipv6 access-list-policers
                                  OOS
NAME                 POLICER NAME  PACKETS
-------------------------------------------
ipv6_p1              10.p1_police  0
ipv6_plp             10.p1_police  0
                     20.p1_police  0
                     30.p2_police  0
```

show sdwan policy rewrite-associations

To display information about rewrite rules to interface bindings on Cisco IOS XE SD-WAN devices, use the **show sdwan policy rewrite-associations** command in privileged EXEC mode.

show sdwan policy rewrite-associations

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

The QoS feature on Cisco IOS XE SD-WAN devices works by examining packets entering at the edge of the network.

Generally, each router on the local service-side network examines the QoS settings of the packets that enter it, determines which class of packets are transmitted first, and processes the transmission based on those settings. As packets leave the network on the remote service-side network, you can rewrite the QoS bits of the packets before transmitting them to meet the policies of the targeted peer router.

You can configure and apply rewrite rules on the egress interface to overwrite the Differentiated Services Code Point (DSCP) value for packets entering the network.

This command can be used to display information about rewrite rules to interface bindings on Cisco IOS XE SD-WAN devices.

Example

The following example shows how to display information about rewrite rules to interface bindings on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan policy rewrite-associations
NAME INTERFACE NAME
transport1 GigabitEthernet0/0/0
transport2 GigabitEthernet0/0/1
```

Related Commands

Command	Description
show sdwan policy access-list-associations	Displays SD-WAN policy access-list-associations.
show sdwan policy access-list-counters	Displays SD-WAN policy access-list-counters.
show sdwan policy access-list-names	Displays SD-WAN policy access-list-names.
show sdwan policy access-list-policers	Displays SD-WAN policy access-list-policers.
show sdwan app-route-policy-filter	Displays information about application-aware routing policy matched packet counts.
show sdwan policy data-policy-filter	Displays SD-WAN policy data-policy-filter.
show sdwan policy from-vsmart	Displays SD-WAN policy from Cisco Catalyst SD-WAN Controller.
show sdwan policy ipv6	Displays SD-WAN policy IPv6.
show sdwan policy service-path	Displays next-hop information for packet coming from service side.
show sdwan policy tunnel-path	Displays next-hop information for packet coming over the WAN tunnel.

show sdwan reboot history

To display the history of when the Cisco vManage device is rebooted, use the **show reboot history** command in privileged EXEC mode. The command displays only the latest 20 reboots.

show sdwan reboot history

Syntax Description

None

Command History

Release	Modification
16.9	Command introduced.

Example

```
Device# show sdwan reboot history
REBOOT DATE TIME           REBOOT REASON
---------------------------------------------------------------------------
2016-03-14T23:24:43+00:00  Initiated by user - patch
2016-03-14T23:36:20+00:00  Initiated by user
2016-03-15T21:06:56+00:00  Initiated by user - activate next-1793
2016-03-15T21:10:11+00:00  Software initiated - USB controller disabled
2016-03-15T21:12:53+00:00  Initiated by user
2016-03-15T23:47:59+00:00  Initiated by user
2016-03-15T23:54:49+00:00  Initiated by user
2016-03-15T23:58:28+00:00  Initiated by user
2016-03-16T00:01:32+00:00  Initiated by user
2016-03-16T00:11:02+00:00  Initiated by user
2016-03-16T00:14:42+00:00  Initiated by user
2016-03-16T00:20:30+00:00  Initiated by user
2016-03-16T00:27:11+00:00  Initiated by user
2016-03-16T00:38:46+00:00  Software initiated - watchdog expired
2016-03-16T00:49:25+00:00  Software initiated - watchdog expired
2016-03-16T01:00:07+00:00  Software initiated - watchdog expired
2016-03-16T03:22:05+00:00  Initiated by user
2016-03-16T03:35:40+00:00  Initiated by user
2016-03-16T21:42:19+00:00  Initiated by user
2016-03-16T22:00:25+00:00  Initiated by user
```

show sdwan running-config

To display the active configuration that is running on devices, use the **details** filter with this command to display the default values for configured components.

show sdwan running-config [*configuration-hierarchy*]

Syntax Description

None	Display the full active configuration.
configuration-hierarchy	Specific Configuration Hierarchy: Display the active configuration for a specific hierarchy in the configuration.

Command History

Release	Modification
16.9	Command introduced.
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	Added **secondary-region** to the output to show the Hierarchical SD-WAN region ID, and **region** to show the secondary region mode. Added **transport-gateway** to the output to indicate the enabled/disabled status. Added **affinity-group** and **affinity-group preference** to the output to indicate the affinity group ID assigned to the device and the preference order.

Usage Guidelines

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.6.1a, edge device accepts template push from Cisco vManage Release 20.6.1 with **integrity-type** configuration. The **show sdwan running-config diff** command fails if the template with **integrity-type** config is pushed from Cisco vManage Release 20.6.1 to older edge devices. Edge device needs to be upgraded to Cisco IOS XE Catalyst SD-WAN Release 17.6.1a or higher version before receiving a template-push from Cisco vManage Release 20.6.1.

Examples

Example 1

```
Device# show sdwan running-config
system
host-name vedge1
system-ip 172.16.255.1
domain-id 1
site-id   1
clock timezone America/Los_Angeles
vbond 10.0.14.4
aaa
  auth-order local radius
  usergroup basic
   task system read write
   task interface read write
  !
  usergroup netadmin
  !
  usergroup operator
   task system read
   task interface read
   task policy read
   task routing read
   task security read
  !
  user admin
   password $1$zvOh58pk$QLX7/RS/F0c6ar94.xl2k.
  !
  user eve
   password $1$aLEJ6jve$aBpPQpkl3h.SvA2dt4/6E/
   group    operator
  !
!
logging
  disk
   enable
  !
 !
!
```

Example 2

```
Device# show sdwan running-config vpn 1
vpn 1
 name ospf_and_bgp_configs
 router
  ospf
   router-id 172.16.255.15
   timers spf 200 1000 10000
   redistribute static
   redistribute omp
```

```
  area 0
   interface ge0/4
   exit
  exit
 !
 pim
  interface ge0/5
  exit
 exit
!
interface ge0/4
 ip address 10.20.24.15/24
 no shutdown
!
interface ge0/5
 ip address 56.0.1.15/24
 no shutdown
!
!
Device# show running-config vpn 1
vpn 1
 name ospf_and_bgp_configs
 no ecmp-hash-key layer4
 router
  ospf
   router-id 172.16.255.15
   auto-cost reference-bandwidth 100
   compatible rfc1583
   distance external 0
   distance inter-area 0
   distance intra-area 0
   timers spf 200 1000 10000
   redistribute static
   redistribute omp
   area 0
    interface ge0/4
     hello-interval      10
     dead-interval       40
     retransmit-interval 5
     priority            1
     network             broadcast
    exit
   exit
  !
  pim
   no shutdown
   no auto-rp
   interface ge0/5
    hello-interval      30
    join-prune-interval 60
   exit
  exit
 !
 interface ge0/4
  ip address 10.20.24.15/24
  flow-control        autoneg
  no clear-dont-fragment
  no pmtu
  mtu                 1500
  no shutdown
  arp-timeout         1200
 !
 interface ge0/5
  ip address 56.0.1.15/24
```

```
  flow-control        autoneg
  no clear-dont-fragment
  no pmtu
  mtu                 1500
  no shutdown
  arp-timeout         1200
 !
!
```

show sdwan security-info

To view the security information configured for IPsec tunnel connections, use the **show sdwan security-info** command in privileged EXEC mode.

show sdwan security-info

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	The output of this command was modified. The `security-info authentication-type` field in the output of this command is deprecated. A new field `security-info integrity-type` field is added to the command output.

Example

The following is a sample output from the **show sdwan security-info** command:

```
Device# show sdwan security-info
security-info authentication-type deprecated
security-info rekey  86400
security-info replay-window 512
security-info encryption-supported "AES_GCM_256 (and AES_256_CBC for multicast)"
security-info fips-mode Disabled
security-info pairwise-keying Disabled
security-info pwk-sym-rekey Enabled
security-info extended-ar-window Disabled
security-info integrity-type ip-udp-esp
```

show sdwan secure-internet-gateway tunnels

To view information about the automatic SIG tunnels that you have configured from a Cisco IOS XE SD-WAN device to Cisco Umbrella or Zscaler SIG, use the **show sdwan secure-internet-gateway tunnels** command in the privileged EXEC mode.

show sdwan secure-internet-gateway tunnels

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 17.9.1a	This command is introduced.

Examples

```
Device# show sdwan secure-internet-gateway tunnels
TUNNEL IF     TUNNEL                                                    HA      DEVICE  SIG
   TRACKER              DESTINATION            TUNNEL
NAME          ID        TUNNEL NAME                                   PAIR    STATE   STATE
  STATE    SITE ID     DATA CENTER  PROVIDER  TYPE    TIMESTAMP
-------------------------------------------------------------------------------------------
Tunnel100001  52615809  site1820851800sys172x16x255x15ifTunnel100001  Active  Up      NA
   Enabled  1820851800  NA           zScaler   IPsec   NA
Tunnel100002  52615814  site1820851800sys172x16x255x15ifTunnel100002  Backup  Up      NA
   Enabled  1820851800  NA           zScaler   IPsec   NA
```

Table 112: Output Columns

Column	Description
TUNNEL IF NAME	Tunnel name configured on the device.
TUNNEL ID	Unique ID for the tunnel defined by the SIG provider.
TUNNEL NAME	Unique name for the tunnel that can be used to identify the tunnel at both the local and remote ends. On the SIG provider portal, you can use the tunnel name to find details about a particular tunnel.
HA PAIR	Active or Backup.
DEVICE STATE	Tunnel status as perceived by the device.
SIG STATE	Tunnel status as perceived by the SIG endpoint. **Note** Supported for Cisco Umbrella SIG endpoints only.
TRACKER STATE	Whether enabled or disabled during tunnel configuration.
SITE ID	ID of the site where the WAN edge device is deployed
DESTINATION DATA CENTER	SIG provider data center to which the tunnel is connected **Note** Supported for Cisco Umbrella SIG endpoints only.
PROVIDER	Cisco Umbrella or Zscaler.
TUNNEL TYPE	IPSec or GRE

show sdwan secure-internet-gateway umbrella tunnels

To view information about the automatic SIG tunnels that you have configured from a Cisco IOS XE SD-WAN device to Cisco Umbrella, use the **show sdwan secure-internet-gateway umbrella tunnels** command in the privileged EXEC mode.

show sdwan secure-internet-gateway umbrella tunnels

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 17.5.1a	This command is introduced.

Examples

```
Device# show sdwan secure-internet-gateway umbrella tunnels
                                                                                                                    API
 LAST
TUNNEL IF                                                                                                           HTTP
 SUCCESSFUL    TUNNEL
NAME          TUNNEL ID  TUNNEL NAME                                FSM STATE             CODE
 REQ           STATE
-------------------------------------------------------------------------------------------------------------------------
Tunnel17447  527398582  SITE10005SYS172x16x255x88IFTunnel17447  st-tun-create-notif  200
 rekey-tunnel  -
Tunnel22427  527398577  SITE10005SYS172x16x255x88IFTunnel22427  st-tun-create-notif  200
 rekey-tunnel  -
Tunnel22457  527398373  SITE10005SYS172x16x255x88IFTunnel22457  st-tun-create-notif  200
 rekey-tunnel  -
```

Table 113: Output Columns

Column	Description
TUNNEL IF NAME	Tunnel name configured on the device.
TUNNEL ID	Unique ID for the tunnel defined by the SIG provider.
TUNNEL NAME	Unique name for the tunnel that can be used to identify the tunnel at both the local and remote ends. On the SIG provider portal, you can use the tunnel name to find details about a particular tunnel.
FSM STATE	The current state of the finite state machine (FSM) when a tunnel is being created to the SIG endpoint.
API HTTP CODE	The last HTTP code received from the SIG endpoint in response to an API request.

Column	Description
LAST SUCCESSFUL REQ	The last API request to the SIG endpoint that was successful.
TUNNEL STATE	Yet to be supported.

show sdwan secure-internet-gateway zscaler tunnels

To view information about the automatic SIG tunnels that you have configured from a Cisco IOS XE SD-WAN device to Zscaler SIG, use the **show sdwan secure-internet-gateway zscaler tunnels** command in the privileged EXEC mode.

show sdwan secure-internet-gateway zscaler tunnels

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 17.5.1a	This command is introduced.

Examples

```
Device# show sdwan secure-internet-gateway zscaler tunnels

                          HTTP
TUNNEL IF                                                 TUNNEL
                                                               LOCATION
                          RESP
NAME           TUNNEL NAME                                ID         FQDN
                                          TUNNEL FSM STATE         ID         LOCATION FSM
STATE    LAST HTTP REQ     CODE
-------------------------------------------------------------------------------------------------------------------------------
Tunnel100001  site1820851800sys172x16x255x15ifTunnel100001  52615809
site1820851800sys172x16x255x15iftunnel100001@example.com  add-vpn-credential-info  52615819
  location-init-state  get-data-centers  200
Tunnel100002  site1820851800sys172x16x255x15ifTunnel100002  52615814
site1820851800sys172x16x255x15iftunnel100002@example.com  add-vpn-credential-info  52615819
  location-init-state  get-data-centers  200
```

Table 114: Output Columns

Column	Description
TUNNEL IF NAME	Tunnel name configured on the device.

Column	Description
TUNNEL NAME	Unique name for the tunnel that can be used to identify the tunnel at both the local and remote ends. On the SIG provider portal, you can use the tunnel name to find details about a particular tunnel.
TUNNEL ID	Unique ID for the tunnel defined by the SIG provider
FQDN	The fully qualified domain name (FQDN) that the device uses to interact with the Zscaler SIG endpoint.
TUNNEL FSM STATE	The current state of the tunnel finite state machine (FSM) when a tunnel is being created to the SIG endpoint.
LOCATION ID	ID provided by Zscaler after the location is set up successfully.
LOCATION FSM STATE	The current state of the location finite state machine (FSM) when a lcation is being set up using Zscaler endpoint APIs.
LAST HTTP REQ	The last API request to the SIG endpoint.
HTTP RESP CODE	The last HTTP code received from the SIG endpoint in response to an API request.

show sdwan software

List the software images that are installed on the local device (on Cisco IOS XE Catalyst SD-WAN devices and vSmart controllers).

show sdwan software *image-name*

show sdwan software

Syntax Description

None	List information about all software images installed on the local device.
image-name	Specific Software Image: List information about a specific software image.

Command History

Release	Modification
16.9	Command introduced.
16.11	Version string displays 5-tuples.
16.12	Includes installer space usage.

Example

Example 1

Release 16.9

```
Device# show sdwan software

VERSION   ACTIVE  DEFAULT  PREVIOUS  CONFIRMED  TIMESTAMP
-------------------------------------------------------------------------------
16.10.2e  true    true     false     user       2022-07-07T23:47:18-00:0
16.9.3    false   true     true      auto       2020-04-08T19:39:36-00:00
```

Example 2

Release 16.12

```
Device# show sdwan software

VERSION          ACTIVE  DEFAULT  PREVIOUS  CONFIRMED  TIMESTAMP
-------------------------------------------------------------------------------
16.10.3.0.0      false   true     true      user       2020-06-08T13:32:21-00:00
17.03.05.0.6600  true    false    false     user       2022-07-19T23:35:54-00:00

Total Space:387M Used Space:130M Available Space:253M
```

show platform software sdwan dta cflowd statistics

To display DTA Cflowd statistics summary, use the **show platform software sdwan dta cflowd statistics** command in privileged EXEC mode.

show patform software sdwan dta cflowd statistics

Syntax Description

dta	Displays DTA information.
cflowd	Displays Cflowd information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.18.1a	This command was introduced.

Examples

The following is a sample output from the **show platform software sdwan dta cflowd statistics** command:

```
device# show platform  software sdwan dta cflowd statistics
DTA FNF Statistics Summary

template_cnt: 0
```

```
data_packets: 11056
template_packets: 123
total_packets: 172
flow_refresh: 30
flow_ageout: 175
flow_end_detected: 0
flow_end_forced: 2
app_aggregation_db_cnt: 0
app_aggregation_aged_cnt: 19
app_aggregation_drop_cnt: 0
app_aggregation_high_watermark: 14
fw_zone_pair: 0
fw_zone: 0
utd_policy: 0
utd_policy_aged: 0
utd_urlf_url: 0
utd_urlf_url_aged: 0
utd_amp_filename: 0
utd_amp_filename_aged: 0
utd_amp_malname: 0
utd_amp_malname_aged: 0
c3pl_class: 0
c3pl_policy: 0
```

show sdwan system status

Display time and process information for the device, as well as CPU, memory, and disk usage data.

show sdwan system status

Syntax Description

None

Command History

Release	Modification
16.9	Command introduced.
17.2	Model name changed to display Cisco IOS XE Catalyst SD-WAN device Product ID.
17.3	Included Hypervisor details.

Examples

Example 1

Release 16.12.4

```
Device# show sdwan system status
Viptela (tm) vedge Operating System Software
Copyright (c) 2013-2020 by Viptela, Inc.
Controller Compatibility: 19.2
Version: 16.12.4.0.4457
```

```
Build: Not applicable

System logging to host is disabled
System logging to disk is enabled

System state: GREEN. All daemons up
System FIPS state: Disabled
Testbed mode: Enabled

Last reboot: Image Install .
CPU-reported reboot: Image
Boot loader version: Not applicable
System uptime: 0 days 02 hrs 18 min 08 sec
Current time: Wed Dec 23 15:26:46 UTC 2020

Load average: 1 minute: 0.15, 5 minutes: 0.12, 15 minutes: 0.13
Processes: 560 total
CPU allocation: 8 total, 1 control, 7 data
CPU states: 1.18% user, 1.39% system, 97.30% idle
Memory usage: 16425460K total, 2302960K used, 14122500K free
330540K buffers, 2548048K cache

Disk usage: Filesystem Size Used Avail Use % Mounted on
/dev/bootflash1 29469M 17656M 10316M 63% /bootflash
/dev/loop18 388M 105M 279M 28% /bootflash/.sdwaninstaller


Personality: vedge
Model name: vedge-ISR-4451-X
Services: None
vManaged: false
Commit pending: false
Configuration template: None
Chassis serial number: FGL174411F8
```

Example 2

Release 17.2.1v

```
Device# show sdwan system status
Viptela (tm) vEdge Operating System Software
Copyright (c) 2013-2020 by Viptela, Inc.
Controller Compatibility: 20.1
Version: 17.02.01v.0.75
Build: Not applicable

System logging to host is disabled
System logging to disk is enabled

System state: GREEN. All daemons up
System FIPS state: Disabled
Testbed mode: Enabled

Last reboot: .
CPU-reported reboot:
Boot loader version: Not applicable
System uptime: 0 days 00 hrs 01 min 38 sec
Current time: Wed Dec 23 16:03:11 UTC 2020

Load average: 1 minute: 2.16, 5 minutes: 1.65, 15 minutes: 0.70
Processes: 515 total
CPU allocation: 8 total, 8 control, 0 data
```

```
CPU states: 11.23% user, 11.19% system, 68.65% idle
Memory usage: 16417952K total, 2432636K used, 13985316K free
305852K buffers, 2573596K cache

Disk usage: Filesystem Size Used Avail Use % Mounted on
/dev/bootflash1 29469M 18987M 8985M 68% /bootflash
387M 140M 242M 37 /bootflash/.installer


Personality: vEdge
Model name: ISR4451-X/K9
Services: None
vManaged: false
Commit pending: false
Configuration template: None
Chassis serial number: FGL174411F8
```

Example 3

17.3.1a

```
Device# show sdwan system status
Viptela (tm) vEdge Operating System Software
Copyright (c) 2013-2020 by Viptela, Inc.
Controller Compatibility: 20.3
Version: 17.03.01a.0.354
Build: Not applicable

System logging to host is disabled
System logging to disk is enabled

System state: GREEN. All daemons up
System FIPS state: Disabled
Testbed mode: Enabled

Last reboot: .
CPU-reported reboot:
Boot loader version: Not applicable
System uptime: 0 days 00 hrs 02 min 13 sec
Current time: Wed Dec 23 16:20:54 UTC 2020

Hypervisor Type: None
Cloud Hosted Instance: false

Load average: 1 minute: 0.94, 5 minutes: 1.64, 15 minutes: 0.81
Processes: 522 total
CPU allocation: 8 total, 8 control, 223 data
CPU states: 10.47% user, 10.48% system, 72.01% idle
Memory usage: 16417952K total, 2245016K used, 14172936K free
316244K buffers, 2566252K cache

Disk usage: Filesystem Size Used Avail Use % Mounted on
/dev/bootflash1 29469M 20330M 7642M 73% /bootflash
387M 159M 224M 41 /bootflash/.installer


Personality: vEdge
Model name: ISR4451-X/K9
Services: None
vManaged: false
Commit pending: false
```

```
Configuration template: None
Chassis serial number: FGL174411F8
```

show sdwan tag-instances from-vsmart

To display the tags downloaded from the Cisco SD-WAN Controller, use the **show sdwan tag-instances from-vsmart** command in privileged EXEC mode.

show sdwan tag-instances from-vsmart

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This command was introduced.

Usage Guidelines

Use the **show sdwan tag-instances from-vsmart** command to show user configuration of tag-instances.

Examples

The following is a sample output from **show sdwan tag-instances from-vsmart** command, displaying tags downloaded from Cisco SD-WAN Controller:

```
Device# show sdwan tag-instances from-vsmart
tag-instances-from-vsmart
 tag-instance APP_facebook_TAG9
  id       60000
  app-list apps_facebook
 tag-instance APP_office_TAG10
  id       70000
  app-list apps_ms apps_zoom
 tag-instance APP_webex_TAG8
  id       50000
  app-list apps_webex
 tag-instance DP_V4_TAG1
  id              10000
  data-prefix-list pfx1
 lists data-prefix-list multicast_pfx
  ip-prefix 224.0.0.0/8
 lists data-prefix-list pfx1
  ip-prefix 10.20.24.0/24
 lists app-list apps_facebook
  app dns
  app facebook
 lists app-list apps_ms
  app ms-office-365
  app ms-office-web-apps
  app ms-services
```

Related Commands

Command	Description
show sdwan policy from-vsmart	Displays policy downloaded from Cisco SD-WAN Controller.

show sdwan version

Display the active version of the Cisco SD-WAN software running on the device.

```
show sdwan version
```

Syntax Description

None

Command History

Release	Modification
16.9	Command introduced.

Example

Example

```
Device# show sdwan version
17.02.01r.0.32
```

show sdwan zbfw drop-statistics

To display zone based firewall drop statistic, use the **show sdwan zbfw drop-statistics** command in privileged EXEC mode.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	This command is supported in Cisco Catalyst SD-WAN

Example

The following example displays the zone based firewall drop statistic.

```
Device#show sdwan zbfw drop-statistics
zbfw drop-statistics catch-all                0
zbfw drop-statistics l4-max-halfsession       0
```

```
zbfw drop-statistics l4-too-many-pkts          0
zbfw drop-statistics l4-session-limit          0
zbfw drop-statistics l4-invalid-hdr            0
zbfw drop-statistics l4-internal-err-undefined-dir 0
zbfw drop-statistics l4-scb-close              0
zbfw drop-statistics l4-tcp-invalid-ack-flag   0
zbfw drop-statistics l4-tcp-invalid-ack-num    0
zbfw drop-statistics l4-tcp-invalid-tcp-initiator 0
zbfw drop-statistics l4-tcp-syn-with-data      0
zbfw drop-statistics l4-tcp-invalid-win-scale-option 0
zbfw drop-statistics l4-tcp-invalid-seg-synsent-state 0
zbfw drop-statistics l4-tcp-invalid-seg-synrcvd-state 0
zbfw drop-statistics l4-tcp-invalid-seg-pkt-too-old 0
zbfw drop-statistics l4-tcp-invalid-seg-pkt-win-overflow 0
zbfw drop-statistics l4-tcp-invalid-seg-pyld-after-fin-send 0
zbfw drop-statistics l4-tcp-invalid-flags      0
zbfw drop-statistics l4-tcp-invalid-seq        0
zbfw drop-statistics l4-tcp-retrans-invalid-flags 0
zbfw drop-statistics l4-tcp-l7-ooo-seg         0
zbfw drop-statistics l4-tcp-syn-flood-drop     0
zbfw drop-statistics l4-tcp-internal-err-synflood-alloc-hostdb-fail 0
zbfw drop-statistics l4-tcp-synflood-blackout-drop 0
zbfw drop-statistics l4-tcp-unexpect-tcp-payload 0
zbfw drop-statistics l4-tcp-syn-in-win         0
zbfw drop-statistics l4-tcp-rst-in-win         0
zbfw drop-statistics l4-tcp-stray-seg          0
zbfw drop-statistics l4-tcp-rst-to-resp        0
zbfw drop-statistics insp-pam-lookup-fail      0
zbfw drop-statistics insp-internal-err-get-stat-blk-fail 0
zbfw drop-statistics insp-dstaddr-lookup-fail  0
zbfw drop-statistics insp-policy-not-present   0
zbfw drop-statistics insp-sess-miss-policy-not-present 0
zbfw drop-statistics insp-classification-fail  0
zbfw drop-statistics insp-class-action-drop    0
zbfw drop-statistics insp-policy-misconfigure  0
zbfw drop-statistics l4-icmp-too-many-err-pkts 0
zbfw drop-statistics l4-icmp-internal-err-no-nat 0
zbfw drop-statistics l4-icmp-internal-err-alloc-fail 0
zbfw drop-statistics l4-icmp-internal-err-get-stat-blk-fail 0
zbfw drop-statistics l4-icmp-internal-err-dir-not-identified 0
zbfw drop-statistics l4-icmp-scb-close         0
zbfw drop-statistics l4-icmp-pkt-no-ip-hdr     0
zbfw drop-statistics l4-icmp-pkt-too-short     0
zbfw drop-statistics l4-icmp-err-no-ip-no-icmp 0
zbfw drop-statistics l4-icmp-err-pkts-burst    0
zbfw drop-statistics l4-icmp-err-multiple-unreach 0
zbfw drop-statistics l4-icmp-err-l4-invalid-seq 0
zbfw drop-statistics l4-icmp-err-l4-invalid-ack 0
zbfw drop-statistics l4-icmp-err-policy-not-present 0
zbfw drop-statistics l4-icmp-err-classification-fail 0
zbfw drop-statistics syncookie-max-dst         0
zbfw drop-statistics syncookie-internal-err-alloc-fail 0
zbfw drop-statistics syncookie-trigger         0
zbfw drop-statistics policy-fragment-drop      0
zbfw drop-statistics policy-action-drop        11
zbfw drop-statistics policy-icmp-action-drop   0
zbfw drop-statistics l7-type-drop              0
zbfw drop-statistics l7-no-seg                 0
zbfw drop-statistics l7-no-frag                0
zbfw drop-statistics l7-unknown-proto          0
zbfw drop-statistics l7-alg-ret-drop           0
zbfw drop-statistics l7-promote-fail-no-zone-pair 0
zbfw drop-statistics l7-promote-fail-no-policy 0
zbfw drop-statistics no-session                0
```

```
zbfw drop-statistics no-new-session            0
zbfw drop-statistics not-initiator             0
zbfw drop-statistics invalid-zone              18
zbfw drop-statistics ha-ar-standby             0
zbfw drop-statistics no-forwarding-zone        0
zbfw drop-statistics backpressure              0
zbfw drop-statistics zone-mismatch             0
zbfw drop-statistics fdb-err                   0
zbfw drop-statistics lisp-header-restore-fail  0
zbfw drop-statistics lisp-inner-pkt-insane     0
zbfw drop-statistics lisp-inner-ipv4-insane    0
zbfw drop-statistics lisp-inner-ipv6-insane    0
zbfw drop-statistics policy-avc-action-drop    0
zbfw drop-statistics l4-icmp-invalid-seq       0
zbfw drop-statistics l4-udp-max-halfsession    0
zbfw drop-statistics l4-icmp-max-halfsession   0
zbfw drop-statistics no-zone-pair-present      0
```

show sdwan zbfw zonepair-statistics

Display zone based firewall zonepair statistics, use the **show sdwan zbfw zonepair-statistics** command in privileged EXEC mode.

show sdwan zbfw zonepair-statistics

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	This command is supported in Cisco Catalyst SD-WAN

Example

The following example displays the zone based firewall zonepair statistics.

```
Device#show sdwan zbfw zonepair-statistics
zbfw zonepair-statistics ZP_zone1_zone1_seq_1
 src-zone-name zone1
 dst-zone-name zone1
 policy-name   seq_1
 fw-traffic-class-entry seq_1-seq-1-cm_
  zonepair-name                  ZP_zone1_zone1_seq_1
  class-action                   Inspect
  pkts-counter                   7236
  bytes-counter                  4573618
  attempted-conn                 9
  current-active-conn            0
  max-active-conn                1
  current-halfopen-conn          0
  max-halfopen-conn              1
  current-terminating-conn       0
  max-terminating-conn           0
  time-since-last-session-create 4373
  fw-tc-match-entry seq_1-seq-rule1-v6-acl_ 3
   match-type "access-group name"
  fw-tc-proto-entry 1
   protocol-name tcp
```

```
  byte-counters 4545768
  pkt-counters  7037
 fw-tc-proto-entry 4
  protocol-name icmp
  byte-counters 27850
  pkt-counters  199
 l7-policy-name                NONE
fw-traffic-class-entry seq_1-seq-11-cm_
 zonepair-name                 ZP_zone1_zone1_seq_1
 class-action                  Inspect
 pkts-counter                  4947
 bytes-counter                 3184224
 attempted-conn                5
 current-active-conn           0
 max-active-conn               1
 current-halfopen-conn         0
 max-halfopen-conn             0
 current-terminating-conn      0
 max-terminating-conn          0
 time-since-last-session-create 4480
 fw-tc-match-entry seq_1-seq-Rule_3-acl_ 3
  match-type "access-group name"
 fw-tc-proto-entry 1
  protocol-name tcp
  byte-counters 3184224
  pkt-counters  4947
 l7-policy-name                NONE
fw-traffic-class-entry class-default
 zonepair-name                 ZP_zone1_zone1_seq_1
 class-action                  "Inspect Drop"
 pkts-counter                  11
 bytes-counter                 938
 attempted-conn                0
 current-active-conn           0
 max-active-conn               0
 current-halfopen-conn         0
 max-halfopen-conn             0
 current-terminating-conn      0
 max-terminating-conn          0
 time-since-last-session-create 0
 l7-policy-name                NONE
```

show sdwan zonebfwdp sessions

To display the existing zone-based firewall sessions on Cisco IOS XE SD-WAN devices, use the **show sdwan zonebfwdp sessions** command in privileged EXEC mode.

show sdwan zonebfwdp sessions

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE SD-WAN Release 17.2.1v	This command is supported in Cisco Catalyst SD-WAN.

Usage Guidelines

Secure SD-WAN brings key security capabilities embedded natively in SD-WAN solution with cloud-based single-pane of management for both SD-WAN and security capabilities. The security capabilities include enterprise firewall with application awareness, intrusion prevention systems with Cisco Talos signatures, URL-Filtering, and DNS/web-layer security.

The Enterprise Firewall with Application Awareness uses a flexible and easily understood zone-based model for traffic inspection.

A firewall policy is a type of localized security policy that allows stateful inspection of TCP, UDP, and ICMP data traffic flows. Traffic flows that originate in a given zone are allowed to proceed to another zone based on the policy between the two zones. A zone is a grouping of one or more VPNs. Grouping VPNs into zones allows you to establish security boundaries in your overlay network so that you can control all data traffic that passes between zones.

Firewall policies can match IP prefixes, IP ports, the protocols TCP, UDP, and ICMP, and applications. Matching flows for prefixes, ports, and protocols can be accepted or dropped, and the packet headers can be logged. Nonmatching flows are dropped by default. Matching applications are denied.

A zone pair is a container that associates a source zone with a destination zone and that applies a firewall policy to the traffic that flows between the two zones.

This command can be used to display the existing zone-based firewall sessions on Cisco IOS XE SD-WAN devices.

Example

The following example shows how to display the existing zone-based firewall sessions on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan zonebfwdp sessions

   SRC  DST                                          TOTAL      TOTAL                   UTD

SESSION                                        SRC    DST                            SRC  DST
  VPN  VPN  ZP      CLASSMAP    NAT    INTERNAL  INITIATOR  RESPONDER  APPLICATION  POLICY

ID       STATE   SRC IP        DST IP        PORT   PORT  PROTOCOL                VRF  VRF
  ID   ID   NAME    NAME        FLAGS  FLAGS     BYTES      BYTES      TYPE         NAME

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

136      open    10.20.24.150  10.1.15.150   39662  1719  PROTO_L7_H225_RAS        1    1
   1    0    in2out  fw-traffic  -      0         166        6                        -

134      open    10.1.15.151   10.20.24.150  5013   5001  PROTO_L7_H323_RTCP_DATA  1    1
   1    0    in2out  fw-traffic  -      0         276        184                      -

132      closed  10.20.24.150  10.1.15.151   48330  1720  PROTO_L7_H323            1    1
   1    0    in2out  fw-traffic  -      65543     506        552                      -

133      open    10.1.15.151   10.20.24.150  5012   5000  PROTO_L7_H323_RTP_DATA   1    1
   1    0    in2out  fw-traffic  -      0         396976     396804                   -
```

show service-insertion type appqoe

To view detailed information about service controllers, service node groups, and individual service nodes, use the **show service-insertion type appqoe** command in privileged EXEC mode.

show service-insertion type appqoe { **status** | **alarms** | **config** | **token** | **cluster-summary** | **appnav-controller-group** | **service-node-group** [*name*] | **service-context** [*service-context-name*] }

Syntax Description

status	Displays the general status of the AppNav-XE controller.
alarms	Displays information about various AppNav-XE controller alarms.
config	Displays AppNav-XE controller configuration.
token	Displays information about the AppNav-XE controller token.
cluster-summary	Displays the summary of the AppNav-XE cluster.
appnav-controller-group	Displays membership details of the AppNav controller group and service nodes configured and registered with the controller group.
service-node-group	Displays configuration details for all service nodes within a service node group.
name	(Optional) Name of the service node group
service-context *service-context-name*	Displays information about all or the specified service context.

Command Default

This command has no default behavior.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	This command was introduced.
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	The output of this command was modified to include sub-service health for AppQoE using the keyword **service-node-group**.

Usage Guidelines

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.6.1a the output of the **show service-insertion type appqoe service-node-group** command shows the sub-service health for AppQoE. However, if the service node runs a version prior to Cisco IOS XE Catalyst SD-WAN Release 17.6.1a, the sub-service health information is unavailable to the service controller. In such cases, the health markers for various AppQoE services show as green with 0% utilization even though not all services may be available to the service nodes.

The following is the sample output from **show service-insertion type appqoe service-node-group** command when the service nodes aren't upgraded to Cisco IOS XE Catalyst SD-WAN Release 17.6.1a:

```
Device# show service-insertion type appqoe service-node-group
Service Node Group name         : SNG-APPQOE
    Service Context             : appqoe/1
    Member Service Node count   : 2


Service Node (SN)                   : 192.0.2.254
Auto discovered                     : No
SN belongs to SNG                   : SNG-APPQOE
Current status of SN                : Alive
System IP                           : 1.0.0.33
Site ID                             : 10050
Time current status was reached              : Tue Apr 20 17:08:29 2021

Cluster protocol VPATH version               : 1 (Bitmap recvd: 1)
Cluster protocol incarnation number          : 1
Cluster protocol last sent sequence number    : 1618944623
Cluster protocol last received sequence number: 392504
Cluster protocol last received ack number     : 1618944622

Health Markers:
              AO       Load State

             tcp          GREEN 0%
             ssl          GREEN 0%
             dre          GREEN 0%
            http          GREEN 0%
```

Example

The following sample output shows the configuration details of service nodes in a service node group:

```
Device# show service-insertion type appqoe service-node-group
Service Node Group name : SNG-APPQOE
Service Context : appqoe/1
Member Service Node count : 2


Service Node (SN) : 10.1.1.1
Auto discovered : No
SN belongs to SNG : SNG-APPQOE
Current status of SN : Alive
System IP : 192.168.1.11
Site ID : 101
Time current status was reached : Wed Sep 23 11:01:49 2020

Cluster protocol VPATH version : 1 (Bitmap recvd: 1)
Cluster protocol incarnation number : 1
Cluster protocol last sent sequence number : 1601432656
Cluster protocol last received sequence number: 715749
Cluster protocol last received ack number : 1601432655
```

The following sample output shows the traffic statistics for service nodes in a service node group:

```
Device# show service-insertion type appqoe statistics service-node-group
Service Node Group: SNG-APPQOE
Number of Service Node(s): 2
Member Service Nodes:
IP Address
10.1.1.1
10.1.1.2

Aggregate of statistics from all SNs of the SNG:
-----------------------------------------------
```

```
Time since statistics were last reset/cleared:

Aggregate number of probe requests sent to SN : 1435070
Aggregate number of probe responses received from SN: 715915
Aggregate number of invalid probe responses received
Total : 0
Incompatible version : 0
Authentication failed : 0
Stale response : 0
Malformed response : 0
Unknown response : 0
Aggregate number of times liveliness was lost with the SN : 1
Aggregate number of times liveliness was regained with the SN:2
Aggregare number of version probes sent to SN: 719033
Aggregate number of version probes received from SN: 2
Aggregate number of healthprobes sent to SN: 716037
Aggregate number of healthprobes received from SN: 715913


Aggregate traffic distribution statistics
-----------------------------------------
Packet and byte counts-
----------------------
Redirected Bytes : 1558757923174
Redirected Packets : 1945422189
Received Bytes : 1582477555093
Received Packets : 1908965233
```

The following sample output shows the configuration details of service controllers in a controller group:

```
Device# show service-insertion type appqoe appnav-controller-group
All AppNav Controller Groups in service context
Appnav Controller Group : ACG-APPQOE
Member Appnav Controller Count : 1
Members:
IP Address
10.1.1.100

AppNav Controller : 192.0.2.1
Local AppNav Controller : Yes
Current status of AppNav Controller : Alive
Time current status was reached : Mon Sep 21 19:09:08 2020
Current AC View of AppNav Controller
IP Address
10.1.1.100

Current SN View of AppNav Controller
IP Address
10.1.1.1
```

show sslproxy statistics

To view SSL proxy statistics and TLS flow counters, use the **show sslproxy statistics** command in privileged EXEC mode.

show sslproxy statistics

Syntax Description

This command has no arguments or keywords.

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	This command was introduced.
Cisco IOS XE Catalyst SD-WAN Release 17.13.1a	This command was modified to include the TLS flow counters in Cisco IOS XE Catalyst SD-WAN Release 17.13.1a.

Example

The following is a sample output from the **show ssl proxy statistics** command showcases SSL statistics and TLS flow counters. The fields are self-explanatory. The count for the TLS flow counter for version 1.3 is shown as 8.

```
Device# show sslproxy statistics
=========================================================
SSL Statistics:
=========================================================
Flow Selected SSL/TLS version:
TLS 1.0 Flows : 0
TLS 1.1 Flows : 0
TLS 1.2 Flows : 0
TLS 1.3 Flows : 8
```

show sslproxy status

To view the status of SSL Proxy, use the **show sslproxy status** command in privileged EXEC mode.

show sslproxy status

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	The command was introduced.
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	The output of this command was modified to remove the fields SSL Proxy Operational State and TCP Proxy Operational State.

Usage Guidelines

Example

The following is sample output from the **show sslproxy status** command.

```
Device# show sslproxy status

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

```
                SSL Proxy Status
============================================================


Configuration
-------------
CA Cert Bundle                : /bootflash/vmanage-admin/bengaluru.pem
CA TP Label                   : PROXY-SIGNING-CA
Cert Lifetime                 : 730
EC Key type                   : P256
RSA Key Modulus               : 2048
Cert Revocation               : NONE
Expired Cert                  : drop
Untrusted Cert                : drop
Unknown Status                : drop
Unsupported Protocol Ver      : drop
Unsupported Cipher Suites     : drop
Failure Mode Action           : close
Min TLS Ver                   : TLS Version 1


Status
------
Clear Mode                    : FALSE
```

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

Field	Description
CA TP label	Default Trustpoint label for SSL proxy.
Cert Lifetime	Certificate lifetime in days.
EC Key type	Enterprise certificate key type for SSL proxy.
RSA Key Modulus	The length of the RSA key. The default key length is 2048.

show standby

To display Hot Standby Router Protocol (HSRP) information, use the **show standby** command in user EXEC or privileged EXEC mode.

show standby [**all** | **brief**]

Syntax Description

all	(Optional) Displays information for groups that are learned or don't have the **standby ip** command configured.
brief	(Optional) Displays a single-line output summarizing each standby group.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE show standby command.

The **no standby** or **no standby version** commands resets the version to 1. If standby IPv6 groups are present on the interface, then the **no standby** command is rejected because v6 groups are not supported with version 1.

You may also observe errors for the standby authentication command with version 1 because authentication isn't supported with the default version.

Examples

The following is a sample output from the **show standby** command:

```
Device# show standby

GigabitEthernet3 - Group 1
 State is Active
   8 state changes, last state change 00:30:53
 Virtual IP address is 12.1.1.100
 Active virtual MAC address is 0000.0c07.ac01 (MAC In Use)
   Local virtual MAC address is 0000.0c07.ac01 (v1 default)
 Hello time 3 sec, hold time 10 sec
   Next hello sent in 0.592 secs
 Preemption disabled
 Active router is local
 Standby router is unknown
 Priority 100 (default 100)
 Group name is "Leader" (cfgd)
 FLAGS: 1/1
 Followed by groups:
   Gi3.1 Grp 1 Active 13.1.1.100 0000.0c07.ac01 refresh 10 secs (expires in 5.728 sec)
```

The following is a sample output from the **show standby** command when HSRP version 2 is configured:

```
Device# show standby
GigabitEthernet0/0/1 - Group 94 (version 2)
```

```
  State is Active
    2 state changes, last state change 01:06:01
    Track object 8 state Up
  Virtual IP address is 10.96.194.1
  Active virtual MAC address is 0000.0c9f.f05e (MAC In Use)
    Local virtual MAC address is 0000.0c9f.f05e (v2 default)
  Hello time 1 sec, hold time 4 sec
    Next hello sent in 0.400 secs
  Authentication MD5, key-string
  Preemption enabled, delay min 180 secs
  Active router is local
  Standby router is 10.96.194.3, priority 105 (expires in 3.616 sec)
  Priority 110 (configured 110)
  Group name is "hsrp-Gi0/0/1.94-94" (default)
  FLAGS: 1/1
GigabitEthernet0/0/1 - Group 194 (version 2)
  State is Active
    2 state changes, last state change 01:06:01
    Track object 80 state Up
  Link-Local Virtual IPv6 address is FE80::5:73FF:FEA0:C2 (impl auto EUI64)
    Virtual IPv6 address 2001:10:96:194::1/64
  Active virtual MAC address is 0005.73a0.00c2 (MAC In Use)
    Local virtual MAC address is 0005.73a0.00c2 (v2 IPv6 default)
  Hello time 1 sec, hold time 4 sec
    Next hello sent in 0.352 secs
  Authentication MD5, key-string
  Preemption enabled, delay min 180 secs
  Active router is local
  Standby router is FE80::2E73:A0FF:FEB3:4AC1, priority 105 (expires in 3.888 sec)
  Priority 110 (configured 110)
  Group name is "hsrp-Gi0/0/1.94-194" (default)
  FLAGS: 1/1
```

The following is a sample output from the **show standby** command using the **brief** keyword:

```
Device# show standby brief
Interface   Grp  Pri P State   Active   Standby           Virtual IP
Gi0/0/1     94   110 P Active  local    10.96.194.3       10.96.194.1
Gi0/0/1     194  110 P Active  local    FE80::2E73:A0FF:FEB3:4AC1    FE80::5:73FF:FEA0:C2
```

The following is a sample output from the **show standby** command when HSRP MD5 authentication is configured:

```
Device# show standby

GigabitEthernet0/0/1 - Group 94 (version 2)
  State is Standby
    1 state change, last state change 01:06:09
    Track object 8 state Up
  Virtual IP address is 10.96.194.1
  Active virtual MAC address is 0000.0c9f.f05e (MAC Not In Use)
    Local virtual MAC address is 0000.0c9f.f05e (v2 default)
  Hello time 1 sec, hold time 4 sec
    Next hello sent in 0.688 secs
  Authentication MD5, key-string
  Preemption enabled, delay min 180 secs
  Active router is 10.96.194.2, priority 110 (expires in 4.272 sec)
    MAC address is cc16.7e8c.6dd1
  Standby router is local
  Priority 105 (configured 105)
  Group name is "hsrp-Gi0/0/1.94-94" (default)
```

The following is a sample output from the **show standby** command when HSRP group shutdown is configured:

```
Device# show standby

Ethernet0/0 - Group 1
State is Init (tracking shutdown)
3 state changes, last state change 00:30:59
Track object 100 state Up
Track object 101 state Down
Track object 103 state Up
```

The following is a sample output from the **show standby** command when HSRP BFD peering is enabled:

```
Device# show standby

Ethernet0/0 - Group 2
  State is Listen
    2 state changes, last state change 01:18:18
  Virtual IP address is 10.0.0.1
  Active virtual MAC address is 0000.0c07.ac02
    Local virtual MAC address is 0000.0c07.ac02 (v1 default)
  Hello time 3 sec, hold time 10 sec
  Preemption enabled
  Active router is 10.0.0.250, priority 120 (expires in 9.396 sec)
  Standby router is 10.0.0.251, priority 110 (expires in 8.672 sec)
    BFD enabled
  Priority 90 (configured 90)
  Group name is "hsrp-Et0/0-1" (default)
```

The following is a sample output from the **show standby** command displaying the state of the standby RP:

```
Device# show standby

GigabitEthernet3/25 - Group 1
State is Init (standby RP, peer state is Active)
Virtual IP address is 10.0.0.1
Active virtual MAC address is unknown
Local virtual MAC address is 0000.0c07.ac01 (v1 default)
Hello time 3 sec, hold time 10 sec
Preemption disabled
Active router is unknown
Standby router is unknown
Priority 100 (default 100)
Group name is "hsrp-Gi3/25-1" (default)
```

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

Table 115: show standby command Field Descriptions

Field	Description
Active router is	Value can be **local**, **unknown**, or an **IP address**. Address (and the expiration date of the address) of the current active hot standby router.
Active virtual MAC address	Virtual MAC address being used by the current active router.
Authentication	Authentication type configured based on the **standby authentication** command.
BFD enabled	Indicates that BFD peering is enabled on the router.

Field	Description
Ethernet - Group	Interface type and number and hot standby group number for the interface.
expires in	Time (in hours:minutes:seconds) in which the standby router will no longer be the standby router if the local router receives no hello packets from it.
Followed by groups:	Indicates the client HSRP groups that have been configured to follow this HSRP group.
Gratuitous ARP 14 sent, next in 7.412 secs	Number of the gratuitous ARP packet HSRP has sent and the time, in seconds, when HSRP sends the next gratuitous ARP packet. This output appears only when HSRP sends gratuitous ARP packets.
Group name is	Name of the HSRP group.
Hello time, hold time	Hello time is the time between hello packets, in seconds, based on the command. The holdtime is the time, in seconds, before other routers declare the active or standby router to be down, based on the **standby timers** command. All the routers in an HSRP group use the hello and hold- time values of the current active router. If the locally configured values are different, the variance appears in parentheses after the hello time and hold-time values.
key-string	Indicates that a key string is used for authentication. Configured key chains aren't displayed.
Local virtual MAC address	Virtual MAC address that will be used if this router became the active router. The origin of this address (displayed in parentheses) can be **default**, **bia** (burned-in address), or **confgd** (configured).
Next hello sent in	Time at which the Cisco IOS software sends the next hello packet (in hours:minutes:seconds).
P	Indicates that the router is configured to preempt.
Preemption enabled, sync delay	Indicates whether preemption is enabled or disabled. If enabled, the minimum delay is the time a higher-priority nonactive router waits before preempting the lower-priority active router. The sync delay is the maximum time a group waits for to synchronize with the IP redundancy clients.
Standby router is	Value can be **local**, **unknown**, or an **IP address**. IP address is the address (and the expiry date of the address) of the “standby” router (the router that is next in line to be the hot standby router).

Field	Description
State is	State of local router. Can be one of the following: • Active: Indicates the current hot standby router. • Standby: Indicates the router that is next in line to be the hot standby router. • Speak: Router is sending packets to claim the active or standby role. • Listen: Router is not in the active or standby state. However, if no messages are received from the active or standby router, it starts to speak. • Init or Disabled: Router isn't yet ready or able to participate in HSRP, possibly because the associated interface isn't up. HSRP groups configured on the other routers on the network, which are learned through snooping, are displayed as being in the initState. Locally configured groups with an interface that is down or groups without a specified interface IP address appear in the initState. For these cases, the Active address and Standby address fields show **unknown**. The state is listed as disabled in the fields when the **standby ip** command hasn't been specified. • Init (tracking shutdown): HSRP groups appear in the initState when HSRP group shutdown is configured and a tracked object goes down.
timeout	Duration (in seconds) for which HSRP accepts message digests based on both the old and new keys.
Tracking	Displays the list of interfaces that are being tracked and their corresponding states based on the configurations, using the **standby track** command.
Virtual IP address is, Secondary virtual IP addresses	All secondary virtual IP addresses are listed on separate lines. If one of the virtual IP addresses is a duplicate of an address configured for another device, it will be marked as **duplicate**. A duplicate address indicates that the router has failed to defend its Address Resolution Protocol (ARP) cache entry.

show standby neighbors

To display information about Hot Standby Router Protocol (HSRP) peer routers on an interface, use the **show standby neighbors** command in privileged EXEC mode.

show standby neighbors [*interface-type interface-number*]

Syntax Description

interface-type interface-number	(Optional) Interface type and number for which output is displayed.

Command Default

HSRP neighbor information is displayed for all the interfaces.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE show standby neighbors command.

Examples

The following is a sample output from the **show standby neighbors** *Ethernet0/0* command displaying the HSRP neighbors on Ethernet interface 0/0. Neighbor 10.0.0.250 is active for group 2 and standby for groups 1 and 8, and is registered with BFD.

```
Device# show standby neighbors Ethernet0/0

HSRP neighbors on Ethernet0/0
  10.0.0.250
    Active groups: 2
    Standby groups: 1, 8
    BFD enabled
  10.0.0.251
    Active groups: 5, 8
    Standby groups: 2
    BFD enabled
  10.0.0.253
    No Active groups
    No Standby groups
    BFD enabled
```

The following is a sample output from the **show standby neighbors** command displaying information for all the HSRP neighbors:

```
Device# show standby neighbors

HSRP neighbors on FastEthernet2/0
  10.0.0.2
    No active groups
    Standby groups: 1
    BFD enabled
HSRP neighbors on FastEthernet2/0
  10.0.0.1
    Active groups: 1
    No standby groups
    BFD enabled
```

The following table describes the significant fields shown in the output.

Table 116: show standby neighbors command Field Descriptions

Field	Description
Active groups	Indicates the HSRP groups for which an interface is acting as the active peer.
Standby groups	Indicates the HSRP groups for which an interface is acting as the standby peer.
BFD enabled	Indicates that HSRP BFD peering is enabled.

show support policy route-policy

To display the control policies configured on a Cisco SD-WAN Controller, use the **show support policy route-policy** command in privileged EXEC mode.

show support policy route-policy

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
	This command was introduced.

Usage Guidelines Use the command on a Cisco SD-WAN Controller. The command output shows the control policies configured on the Cisco SD-WAN Controller, and the TLOCs associated with each control policy.

Example

The following example shows information for a single policy, including the TLOCs of interest.

```
vsmart# show support policy route-policy

================================
  ROUTE POLICIES
================================

route-policy hub-and-spoke-v1
seq-num 46
users-count 1
action srvc/srvc-chain/tloc/tloc-list/affinity counts: 0/0/0/1/0
Policy TLOC-Interest Database:
   TLOC:172.16.255.11 : lte : ipsec Ref-Count: 1

    sequence: 1
        match tloc [SITE-LIST  (0x1) ]
            site-list: HUB (0x1234567890ab)
        action: accept
        set: [ (0x0) ]
    sequence: 11
        match route [PFX-LIST  (0x10) ]
            IPv4 prefix-list: ALL-ROUTES (0x2345678901ab)
        action: accept
        set: [TLOC-LIST  (0x20) ]
            tloc-list: HUB-TLOCS [none]
    default-action: reject, fetch_xml: 1

  Users:
  172.16.255.14, type: route, dir: out, policy: hub-and-spoke-v1 (0x3456789012ab), ctx:
0x4567890123ab, cb: 0x5678901234ab, change: no
```

show tech-support sdwan bfd

To display BFD information on Cisco IOS XE Catalyst SD-WAN devices, use the **show tech-support sdwan bfd** command in privileged EXEC mode.

show tech-support sdwan bfd [detail]

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	This command was introduced.

Usage Guidelines

The **show tech-support sdwan bfd** command displays BFD information about devices for troubleshooting. The command displays the output of the following **show** commands:

- show sdwan bfd summary
- show platform software sdwan session
- show platform software bfd f0 summary
- show platform hardware qfp active feature bfd datapath sdwan summary
- show platform hardware qfp active feature sdwan datapath session summary

The **show tech-support sdwan bfd detail** command displays detailed BFD information about devices for troubleshooting. With the **detail** keyword, the command displays the output of the following commands:

- show sdwan bfd sessions
- show platform software sdwan session
- show platform software sdwan session adj
- show platform software ipsec ftm-msg-stats
- show platform software bfd f0
- show platform software object-manager f0 statistics
- show platform software ipsec f0 flow table
- show platform hardware qfp active feature bfd datapath sdwan all
- show platform hardware qfp active feature bfd datapath statistics

Example 1

The following is a sample output from the **show tech-support sdwan bfd** command.

```
Device#show tech-support sdwan bfd

------------------ show sdwan bfd summary ------------------

sessions-total           12
sessions-up              12
sessions-max             12
sessions-flap            2
poll-interval            600000
sessions-up-suspended    0
sessions-down-suspended  0

------------------ show platform software sdwan session ------------------
======Session Database=====
RemoteSysIP         Color               Proto SrcIp               SPort DstIp
  DPort DPubIp              PPort BFD-LD TUN-ID SA-ID     WAN-Intf (nexthop)
10.1.1.21           metro-ethernet      IPSEC 10.10.1.129         12346 10.10.1.121
  12386 10.10.1.121        12386 20011  11     603979798 GigabitEthernet0/0/1 (10.10.1.121)
10.1.1.23           metro-ethernet      IPSEC 10.10.1.129         12346 10.10.1.123
  12426 10.10.1.123        12426 20009  9      603979794 GigabitEthernet0/0/1 (10.10.1.123)
...

------------------ show platform software bfd f0 ------------------
Forwarding Manager BFD Information
Local Discri   If Handle         Src IP            Dst IP        Encap      AOM ID    Status

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

   20001          0x8         10.10.1.129       10.10.1.130      IPSEC       403       Done

   20002          0x8         10.10.1.129       10.10.1.135      IPSEC       404       Done

...

------------------ show platform hardware qfp active feature bfd datapath sdwan summary
-----------
Total number of session: 12
LD       SrcIP             DstIP         TX          RX      Encap      State     AppProbe
    AdjId
20001  10.10.1.129     10.10.1.130     23973      23971      IPSEC      Up        YES
 GigabitEthernet0/0/1 (0xf800005f)
20002  10.10.1.129     10.10.1.135     22769      22766      IPSEC      Up        YES
 GigabitEthernet0/0/1 (0xf800006f)
...

------------------ show platform hardware qfp active feature sdwan datapath session summary
 ---------
Src IP          Dst IP          Src Port Dst Port   Encap    Uidb     Bfd Discrim PMTU
 Flags
------          ------          -------- -------    ------   -------  ----------- -----
 -----
10.10.1.129     10.10.1.71      12346    12346      CTRL     0        0           0
 0x0
10.10.1.129     10.10.1.125     12346    12406      IPSEC    65527    20004       1442
 0x0
...
```

Example 2

The following is a sample output from the **show tech-support sdwan bfd detail** command.

```
Device#show tech-support sdwan bfd detail

------------------ show sdwan bfd sessions ------------------
                                      SOURCE TLOC      REMOTE TLOC
             DST PUBLIC                       DST PUBLIC         DETECT      TX

SYSTEM IP        SITE ID     STATE       COLOR            COLOR            SOURCE IP
                                 IP                                              PORT
   ENCAP  MULTIPLIER  INTERVAL(msec  UPTIME          TRANSITIONS
-------------------------------------------------------------------------------------
10.1.1.21        121         up          metro-ethernet   default          10.10.1.129
                                 10.10.1.121                                     12386
   ipsec  7           1000           0:01:30:24      1
10.1.1.23        123         up          metro-ethernet   public-internet  10.10.1.129
                                 10.10.1.123                                     12426
   ipsec  7           1000           0:02:50:15      0
...

------------------ show platform software sdwan session ------------------

======Session Database=====
RemoteSysIP         Color               Proto SrcIp               SPort DstIp
  DPort DPubIp              PPort BFD-LD TUN-ID SA-ID     WAN-Intf (nexthop)
10.1.1.21           metro-ethernet      IPSEC 10.10.1.129         12346 10.10.1.121
  12386 10.10.1.121        12386 20011  11     603979798 GigabitEthernet0/0/1 (10.10.1.121)
10.1.1.23           metro-ethernet      IPSEC 10.10.1.129         12346 10.10.1.123
  12426 10.10.1.123        12426 20009  9      603979794 GigabitEthernet0/0/1 (10.10.1.123)
...

------------------ show platform software sdwan session adj ------------------

============  Adjacency Database =============
Index  Interface           IP address       Same-Cable  is-p2p  adj-exist resolved
ref-count      handle
(0):   GigabitEthernet0/0/1(8),       10.10.1.130,     1,          0,       1,       1,
       1,             0x7F543F07B518
(1):   GigabitEthernet0/0/1(8),       10.10.1.135,     1,          0,       1,       1,
       1,             0x7F543F07A5C8
...

------------------ show platform software ipsec ftm-msg-stats ------------------

            MSG Type   From FTM   Suppressed        OK        ERR
            CREATE         12            0        12         0
            DELETE          0            0         0         0
         REKEY(IN)          0            0         0         0
        REKEY(OUT)          1            0         1         0

           Ring Name      Read    Write   ReadERR  WriteERR ItemCount
           DCR Ring          0        0         0         0         0
           DDM Ring          0        0         0         0         0
 ftm_msg_rate(per second) 100

------------------ show platform software bfd f0 ------------------

Forwarding Manager BFD Information

Local Discri   If Handle         Src IP           Dst IP        Encap      AOM ID    Status

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

   20001          0x8         10.10.1.129       10.10.1.130      IPSEC       403      Done

   20002          0x8         10.10.1.129       10.10.1.135      IPSEC       404      Done
```

```
...

------------------ show platform software object-manager f0 statistics ------------------

Forwarding Manager Asynchronous Object Manager Statistics

Object update: Pending-issue: 0, Pending-acknowledgement: 0
Batch begin:   Pending-issue: 0, Pending-acknowledgement: 0
Batch end:     Pending-issue: 0, Pending-acknowledgement: 0
Command:       Pending-acknowledgement: 0
Total-objects: 560
Stale-objects: 0
Resolve-objects: 0
Childless-delete-objects: 0
Backplane-objects: 0
Error-objects: 0
Number of bundles: 0
Paused-types: 3

------------------ show platform software ipsec f0 flow table ------------------

Flow id  QFP SA hdl  SPI         local IP                                lport  remote IP
                               rport  dir       proto  mode
-------------------------------------------------------------------------------------------
1        6           0x000102    10.10.1.129                           12346  10.10.1.130
                               12406  inbound   esp    transport
2        26          0x000255    10.10.1.129                           12346  10.10.1.130
                               12406  outbound  esp    transport
...

------------------ show platform hardware qfp active feature bfd datapath sdwan all
------------------

Total number of session: 12

LD                    : 20001
My Private IP         : 10.10.1.129
Remote Private IP     : 10.10.1.130
Tx Stats              : 24060
Rx Stats              : 24058
Encap Type            : IPSEC
State                 : Up
AppProbe              : YES
IPSec Out SA ID       : 603979778
Tunnel Rec ID         : 1
IfName                : GigabitEthernet0/0/1 (0xf800005f)
Uidb                  : 65528
Config Tx Timer       : 1000000
Conig Detect Timer    : 7000000
Actual Tx Timer       : 1000000
Actual Detect Timer   : 7000000
My Pub IP             : 10.10.1.129
My Pub Port           : 12346
My Symmetric NAT IP   : 0.0.0.0
My Symmetric NAT Port : 0
Remote public IP      : 10.10.1.130
Remote public Port    : 12406
MTU(config), Actual   : 1442, 1442
Farend PMTU           : 1442
My Capabilities       : 0x160
Remote Capabilities   : 0x160
SDWAN BFD flags       : ||||
local_color           : 3
```

```
Ipsec Overhead        : 38
PFR stats for SLA default (addr:df297530)
 Number of pkts  : 30
 Loss Count      : 0
 Latency(1/16ms) : 416
 Jitter(1/16ms)  : 96
Following are SDWAN stats
 Echo Tx         : 23829
 Echo Rx         : 23827
 PMTU Tx         : 231
 PMTU RX         : 231
AppProbeID  Valid  NextProbeID    StatAddr    #Packets    Loss   Latency(1/16ms)
Jitter(1/16ms)
    1         N         0         df297548           0       0                  0
       0
    2         N         0         df297560           0       0                  0
       0
...

------------------ show platform hardware qfp active feature bfd datapath statistics
------------------
QFP BFD global statistics

CPP num: 0
 Data Path IPC Statistics:
  IPC Tx: 31, IPC Rx: 31

 Data Path Session Statistics:
  Session Added: 12, Removed: 0
  Session Up: 12, Down: 0, Init: 0

 Data Path Memory Chunk Statistics:
  Alloc: 12, Free: 0, Fail: 0
  Chunk Add: 0, Return: 0

 Data Path BFD ingress packets Statistics:
  Total receive: 272567, Punt to PI: 0
  Drop due to error: 0, Consume normally: 0

 Data Path BFD SDWAN packets Statistics:
  PktSb Not Found: 0, No Bfd session: 0, Bfd AdminDown: 0
  BFD Corrupted TLV: 0, BFD No TLV: 0
  No Tunnel Adj: 0, Invalid Adj2: 0, Physical Adj Invalid: 0
  Pmtu tx error: 0, Pmtu rx error: 0, Pmtu disabled: 14
  Echo Tx error: 0, Echo Rx error: 0
  tloc ipc: 0, Pmtu ipc: 12, Bfd state ipc: 16, bfd timer ipc: 0
  Oce chain invalid: 0
```

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 *track-number* [**brief** | **interface** [**brief**] | **ip** [**route** | **sla**] [**brief**] | **application** [**brief**] | **WORD** [**map**] | **stub-object** [**brief**] | **service** [**brief**] | **resolution** | **summary** | **timers**]

Syntax Description

track-number	(Optional) Specifies the track number that is being tracked. The range is from 1 to 1000.
WORD	(Optional) Displays track object string.
map	(Optional) Displays track object map information.
application	(Optional) Displays application objects.
brief	(Optional) Displays a single line of information related to the preceding argument or keyword.
endpoint-tracker	(Optional) Displays endpoint object tracker.
interface	(Optional) Displays interface objects.
iproutesla	(Optional) Displays tracked IP route or sla objects.
ipv6route	(Optional) Displays tracked IPv6 route objects.
resolution	(Optional) Displays resolution of ipv4 or ipv6 tracked parameters.
service	(Optional) Displays service objects.
timers	(Optional) Displays polling interval timers.

Command Default

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE show track command.

Example

The following is a sample output from the **show track** command:

```
Device# show track 8
Track 8
  IP route 0.0.0.0 0.0.0.0 reachability
  Reachability is Up (OMP)
    10 changes, last change 1w3d
  VPN Routing/Forwarding table "509"
  First-hop interface is Sdwan-system-intf
  Tracked by:
    HSRP GigabitEthernet0/0/1.94 94
    Track List 7
```

show uidp statistics

To display UIDP statistics, use the **show uidp statistics** command in privileged EXEC mode.

show uidp statistics

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This command was introduced.

Examples

The following sample output displays UIDP statistics.

```
Device# show uidp statistics
Add/Delete Stats
---------------------------------------
Total Users added            : 22
Total Usergroups added       : 12
Total SGT added              : 0
Total Users deleted          : 0
Total Usergroups deleted     : 0
Total SGT deleted            : 0
---------------------------------------
 Add/Delete Error Stats
---------------------------------------
 User add error              : 0
 Usergroup add error         : 0
 SGT add error               : 0
 User delete error           : 0
 Usergroups delete error     : 0
 SGT delete error            : 0
---------------------------------------
 Memory allocation error Stats
---------------------------------------
 ipvrf key list create error : 0
 Index list create error     : 0
 Memory allocation error     : 0
 Invalid binding event       : 0
-----------------------------------------------
 DB Add/Delete Bindings stats
-----------------------------------------------
 Total IP User binding added             : 341
 Total IP User binding delete            : 0
 Total IP User binding add error         : 0
 Total IP User binding delete error      : 0
 Total User Usergroups binding added        : 20
 Total User Usergroups binding deleted      : 0
 Total User Usergroups binding add error    : 0
 Total User Usergroups binding delete error : 0
```

Related Commands

Command	Description
show uidp user-group all	Displays UIDP user group info.
show uidp user ip	Displays the user information by IP address.

show uidp user-group all

To display UIDP user group information, use the **show uidp user-group all** command in privileged EXEC mode.

show uidp user-group all

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This command was introduced.

Examples

The following sample output displays UIDP user group info.

```
Device# show uidp user-group all
Total Usergroups : 12
-------------------------
SDWAN-IDENTITY.CISCO.COM/Builtin/Users
User Identity Groups:Employee
User Identity Groups:TestUserGroup-1
null
Unknown
sdwan-identity.cisco.com/S-1-5-32-545
S-1-5-21-787885371-2815506856-1818290038-513
SDWAN-IDENTITY.CISCO.COM/Users/Domain Users
cisco
eng
dev
mgmt
cEdge-identity#
cEdge-identity#sh uidp user-group us
cEdge-identity#sh uidp user ?
  all   Show all users info
  ip    Show user info by ip
  name  Show user info by user name
```

Related Commands

Command	Description
show uidp statistics	Displays UIDP statistics.
show uidp user ip	Displays the user information by IP address.

show uidp user ip

To display the user information by IP address, use the **show uidp user ip** command in privileged EXEC mode.

show uidp user ip

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This command was introduced.

Examples

The following sample output displays the user information by IP address.

```
Device# show uidp user ip
 User Info 1 : TestUser0@SDWAN-IDENTITY.CISCO.COM
cEdge-identity#sh uidp user name TestUser0@SDWAN-IDENTITY.CISCO.COM
------------------------------------------------------------------------------
User Id    User Name                          IP address
    VRF   Usergroup  Usergroup Name
------------------------------------------------------------------------------
1           TestUser0@SDWAN-IDENTITY.CISCO.COM   72.1.1.7
    0     1          SDWAN-IDENTITY.CISCO.COM/Builtin/Users

          5          Unknown

          6          sdwan-identity.cisco.com/S-1-5-32-545

          7          S-1-5-21-787885371-2815506856-1818290038-513

          8          SDWAN-IDENTITY.CISCO.COM/Users/Domain Users
```

Related Commands

Command	Description
show uidp statistics	Displays UIDP statistics.
show uidp user-group all	UIDP user group information.

show utd engine standard config

To display the Unified Threat Defense (UTD) configuration, use the **show utd engine standard config** command in user EXEC mode.

show utd engine standard config

Command Default None

Command Modes

User EXEC (>)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	This command was introduced.

Examples

The following sample output displays the unified threat defense (UTD) configuration.

```
Device# show utd engine standard config
TD Engine Standard Configuration:


Unified Policy: Enabled


URL-Filtering Cloud Lookup: Enabled


URL-Filtering On-box Lookup: Disabled


File-Reputation Cloud Lookup: Disabled


File-Analysis Cloud Submission: Disabled


UTD TLS-Decryption Dataplane Policy: Enabled


Flow Logging: Disabled


UTD VRF table entries:

Policy: uni-utd

 Threat Profile: uips


VirtualPortGroup Id: 1


UTD threat-inspection profile table entries:

Threat profile: uips

 Mode: Intrusion Prevention
```

```
 Policy: Balanced

 Logging level: Error


UTD threat-inspection whitelist profile table entries:

 UTD threat-inspection whitelist profile table is empty


UTD web-filter profile table entries

 UTD web-filter profile table is empty


UTD TLS-Decryption profile table entries

 UTD TLS-Decryption profile table is empty


UTD File analysis table entries

 UTD File analysis profile table is empty


UTD File reputation table entries

 UTD File reputation profile table is empty
```

show utd unified-policy

To display the unified policy configuration, use the **show utd unified-policy** command in user EXEC mode.

show utd unified-policy

Command Default

None

Command Modes

User EXEC (>)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	This command was introduced.

Examples

The following sample output displays the unified policy configuration.

```
Device# show utd unified-policy
Unified Policy is enabled
```

```
Config State : MT Config Sync Complete

Bulk download Timer State  : Stopped

Messages sent in current transaction: 0

Config download queue size: 0

UTD TLS-decryption dataplane policy is enabled
```

show vrrp

To display the status of configured Virtual Router Redundancy Protocol (VRRP) groups on a device, use the **show vrrp** command in privileged EXEC mode.

show vrrp *group number* [**GigabitEthernet** | **ipv4** | **all** | **brief** | **detail** | **statistics**]

Syntax Description

group number	VRRP group number. The range is from 1–255.
GigabitEthernet	(Optional) Displays GigabitEthernet information for IEEE 802.3z.
ipv4	(Optional) Displays information about IPv4 groups.
all	(Optional) Displays information about all VRRP groups, including groups in a disabled state.
brief	(Optional) Displays a summary view of the VRRP group information.
detail	(Optional) Displays information about all VRRP groups, including statistical information.
statistics	(Optional) Displays statistical information about the VRRP groups.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command is supported for Cisco Catalyst SD-WAN.

Usage Guidelines

If no group is specified, the status for all groups is displayed.

For usage guidelines, see the Cisco IOS XE show vrrp command.

Examples

The following is a sample output from the **show vrrp detail** command:

```
Device# show vrrp detail
GigabitEthernet2 - Group 1 - Address-Family IPv4
 State is BACKUP
 State duration 2 hours 13 mins 4 secs
 Virtual IP address is 10.10.1.10
 Virtual MAC address is 0000.5E00.0101
 Advertisement interval is 1000 msec
```

```
 Preemption enabled
 Priority is 100
    Track object 1 state UNDEFINED decrement 10
 Router is 10.1.1.1, priority is 180
 Master Advertisement interval is 1000 msec (learned)
 Master Down interval is 3609 msec (expires in 3319 msec)
 tloc-change increase-preference 333 configured
 FLAGS: 1/1
```

The following is a sample output from the **show vrrp** command:

```
Device# show vrrp
Ethernet1/0 - Group 1
State is Master
Virtual IP address is 10.2.0.10
Virtual MAC address is 0000.5e00.0101
Advertisement interval is 3.000 sec
Preemption is enabled
 min delay is 0.000 sec
Priority 100
 Track object 1 state down decrement 15
Master Router is 10.2.0.1 (local), priority is 100
Master Advertisement interval is 3.000 sec
Master Down interval is 9.609 sec
Ethernet1/0 - Group 2
State is Master
Virtual IP address is 10.0.0.20
Virtual MAC address is 0000.5e00.0102
Advertisement interval is 1.000 sec
Preemption is enabled
 min delay is 0.000 sec
Priority 95
Master Router is 10.0.0.1 (local), priority is 95
Master Advertisement interval is 1.000 sec
Master Down interval is 3.628 sec
```

The following is a sample output from the **show vrrp** command, displaying peer RP state information:

```
Device# show vrrp
Ethernet0/0 - Group 1
  State is Init (standby RP, peer state is Master)
  Virtual IP address is 172.24.1.1
  Virtual MAC address is 0000.5e00.0101
  Advertisement interval is 1.000 sec
  Preemption enabled
  Priority is 255
  Master Router is 172.24.1.1 (local), priority is 255
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.003 sec
```

The following is a sample output from the **show vrrp** command, displaying information about a configured VRRS group name:

```
Device# show vrrp
GigabitEthernet0/0/0 - Group 1
 State is Master
 Virtual IP address is 10.0.0.7
 Virtual MAC address is 0000.5e00.0101
 Advertisement interval is 1.000 sec
 Preemption enabled
 Priority is 100
 VRRS Group name CLUSTER1 ! Configured VRRS Group Name
```

```
 Master Router is 10.0.0.1 (local), priority is 100
 Master Advertisement interval is 1.000 sec
 Master Down interval is 3.609 sec
```

The following is a sample output from the **show vrrp** command, displaying information when an object is being tracked:

```
Device# show vrrp
Ethernet0/0 - Group 1 - Address-Family IPv4
  State is BACKUP
  State duration 1 mins 41.856 secs
  Virtual IP address is 172.24.1.253
  Virtual MAC address is 0000.5E00.0101
  Advertisement interval is 1000 msec
  Preemption enabled
  Priority is 80 (configured 100)
    Track object 1 state Down decrement 20
  Master Router is 172.24.1.2, priority is 100
  Master Advertisement interval is 1000 msec (learned)
  Master Down interval is 3609 msec (expires in 3297 msec)
```

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

Table 117: show vrrp command Field Descriptions

Field	Description
Ethernet1/0 - Group	Interface type and number, and VRRP group number.
State is	Role this interface plays within VRRP (master or backup).
Advertisement interval is	Interval at which the device sends VRRP advertisements when it is the master virtual device. This value is configured with the **vrrp timers advertise** command.
Priority	Priority of the interface.
Track object	Object number representing the object to be tracked.
state	State value (up or down) of the object being tracked.
decrement	Amount by which the priority of the device is decremented (or incremented) when the tracked object goes down (or comes back up).
Master Router is	IP address of the current master virtual device.
priority is	Priority of the current master virtual device.
Master Advertisement interval is	Advertisement interval, in seconds, of the master virtual device.

Field	Description
Master Down interval is	Calculated time, in seconds, that the master virtual device can be down before the backup virtual device takes over.

The following is a sample output from the **show vrrp brief** command:

```
Device# show vrrp brief
Interface    Grp  A-F Pri   Time Own Pre  State   Master addr/Group addr
  Et1/0       1   IPv4 150    0   N   Y   MASTER  10.0.0.1(local) 10.0.0.10
  Et1/0       1   IPv6 100    0   N   Y   INIT    AF-UNDEFINED no address
  Et1/0       6   IPv6 150    0   N   Y   MASTER  FE80::1(local) FE80::100
```

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

Table 118: show vrrp brief command Field Descriptions

Field	Description
Interface	Interface type and number.
Grp	VRRP group to which this interface belongs.
Pri	VRRP priority number for this group.
Time	Calculated time that the master virtual device can be down before the backup virtual device takes over.
Own	IP address owner.
Pre	Preemption status. Y indicates that preemption is enabled. If this field is empty, preemption is disabled.
State	Role this interface plays within VRRP (master or backup).
Master addr	IP address of the master virtual device.
Group addr	IP address of the virtual device.

show wireless-bridge status

To view details about of a wireless interface module, use the **show wireless-bridge status** command in privileged EXEC (#) mode.

show wireless-bridge status

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.14.1a	This command is supported in Cisco Catalyst SD-WAN.

Examples

The following is a sample output from the **show wireless-bridge status** command.

```
Device# show wireless-bridge status
Module Operating Mode : WGB mode
Module Status         : Module State Ready
Software Version      : 17.17.0.59
Module Session Status : Login Success
```

show wireless-lan radio

To display the radio parameters of the wireless LAN, use the **show wireless-lan radio** command in user EXEC mode.

show wireless-lan radio

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

User EXEC (>)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	This command was introduced.

Examples

The following sample output displays the radio parameters of the wireless LAN.

```
Device# show wireless-lan radio

band  admin  oper  TxPwr  Channel
 ----  -----  ----  -----  --------------------
 2.4g     on    up   2dbm  1
  5g      on    up   2dbm  100,104,108,112
```

show wireless-lan wlan

To display information about the wireless SSID, use the **show wireless-lan wlan** command in user EXEC mode.

show wireless-lan wlan

Syntax Description

This command has no keywords or arguments.

Command Default None

Command Modes User EXEC (>)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	This command was introduced.

Examples The following sample output displays information about the wireless SSID.

```
Device# show wireless-lan wlan

  wlan  oper  vlan  #client  SSID
 ----  ----  ----  -------  -----------------
    1    up    19        0  119
    2    up   105        0  122
    3    up    23        0  123
    4    up   100        0  hello
    5    up    22        0  hello2
```

show wireless-lan client

To display information about the wireless clients in a wireless LAN, use the **show wireless-lan client** command in user EXEC mode.

show wireless-lan client

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes User EXEC (>)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	This command was introduced.

Examples The following sample output displays information about the wireless clients in the wireless LAN.

```
Device# show wireless-lan client

 Client-MAC-Addr    band  status        SSID
 -----------------  ----  ------------  -------------
 64:BC:0C:65:8B:4C    5g  Associated    hello
```

show zone-pair security

To display the source zone, destination zone, and policy attached to the zone-pair, use the **show zone-pair security** command in privileged EXEC mode.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	This command is supported in Cisco Catalyst SD-WAN

Usage Guidelines

For usage guidelines, see the Cisco IOS XE show zone-pair security command.

Example

The following example displays the source zone, destination zone, and policy attached to the zone-pair.

```
Device#show zone-pair security
Zone-pair name ZP_zone1_zone1_seq_1 1
    Source-Zone zone1  Destination-Zone zone1
    service-policy seq_1
```

verify

To verify the file integrity of a software image stored in the device bootflash, use the **verify** command in privileged EXEC mode.

verify *image*

Syntax Description

image	Software image stored in the device bootflash. Specify the file as follows: **bootflash:***filename*

Command Default

This command has no default behavior.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Example

```
Device# verify bootflash:image.bin
Verifying file integrity of
```

```
Embedded Hash   SHA1 : 0123456789ABCDEF0123456789ABCDEF01234567
Computed Hash   SHA1 : 0123456789ABCDEF0123456789ABCDEF01234567
Starting image verification
Hash Computation:    100%Done!
Computed Hash   SHA2: 0123456789abcdef0123456789abcdef
                      0123456789abcdef0123456789abcdef
                       0123456789abcdef0123456789abcdef
                       0123456789abcdef0123456789abcdef

Embedded Hash   SHA2: 0123456789abcdef0123456789abcdef
                       0123456789abcdef0123456789abcdef
                       0123456789abcdef0123456789abcdef
                       0123456789abcdef0123456789abcdef

Digital signature successfully verified in file bootflash:image.bin
```

vdiagnose vmanage cluster

To run diagnostics on a Cisco SD-WAN Manager cluster, use the **vdiagnose vmanage cluster** command in privileged EXEC mode on Cisco SD-WAN Manager.

vdiagnose vmanage cluster [*verbose*]

Syntax Description

cluster	Run diagnostics on a Cisco SD-WAN Managercluster.
verbose	(Optional) View a verbose version of the **vdiagnose vmanage cluster** command.

Command Default

None

Command Modes

Privileged EXEC mode (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	This command is supported in Cisco Catalyst SD-WAN.

Usage Guidelines

Run the **vdiagnose vmanage cluster** command directly from the CLI on any Cisco SD-WAN Manager node in a cluster.

The **vdiagnose vmanage cluster** command tests the following for a Cisco SD-WAN Manager cluster:

- **Mandatory interfaces operational status**: Tests the operational status of the cluster interface on a Cisco SD-WAN Manager node.
- **Cluster interface reachability:** Runs a ping test on all cluster node interfaces in a network, verifying full interface reachability across all Cisco SD-WAN Manager nodes.
- **Cluster services health status:** Provides the health status of cluster services running on one or more Cisco SD-WAN Manager nodes.

- **Cluster service reachability:** Performs nping test for cluster services running on Cisco SD-WAN Manager nodes in the cluster.
- **Current node container status:** Provides the docker container status of cluster services running on the current Cisco SD-WAN Manager node.

Perform the following steps to run the **vdiagnose vmanage cluster** diagnostics command from the CLI on any Cisco SD-WAN Manager node in a cluster:

1. From the Cisco SD-WAN Manager menu, choose **Tools** > **SSH Terminal**.
2. Choose **vManage** as the device in the left pane. The **SSH Terminal** window opens in the right pane.
3. Enter the username and password to log in to Cisco SD-WAN Manager.
4. Enter the **vdiagnose vmanage cluster** command to run a diagnostic test on a Cisco SD-WAN Manager cluster.
5. (Optional) Enter the **vdiagnose vmanage cluster verbose** command to view the verbose of the diagnostic test executed on a Cisco SD-WAN Manager cluster.

Example

The following example shows the results of the diagnostics run on a Cisco SD-WAN Manager controller to test a Cisco SD-WAN Manager cluster:

```
Device#vdiagnose vmanage cluster
Running vdiagnostics, this can take some time...
Current Date and time is 2023-08-03 15:37:02.897422


Personality is Vmanage
Running vdiagnostics for Cluster, this can take some time..

Current node: 10.0.105.39

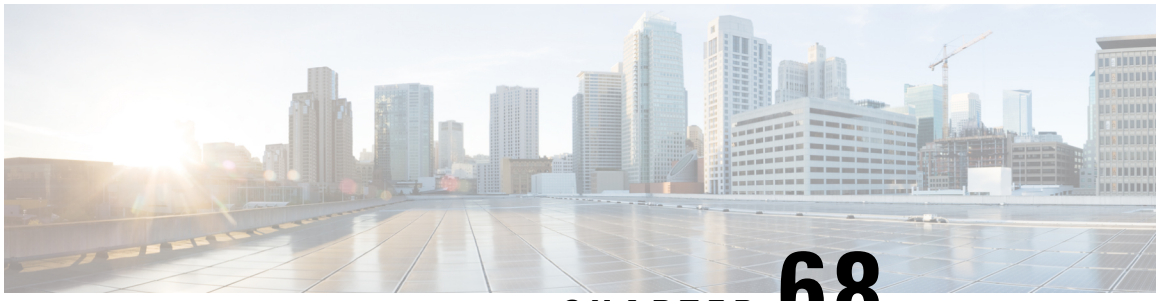
Checking interfaces operational status
======================================
        eth5 - Cluster                                                  PASS

Checking cluster interface reachability
=======================================
        Full interface reachability across all nodes                    PASS

Checking services health status
===============================
        Services healthy across all nodes                               PASS

Checking service reachability
=============================
        Full service reachability across all nodes                      PASS

Checking current node container status
======================================
        All cluster services containers are up                          PASS
```



CHAPTER 68

Wireless Commands

- passphrase, on page 1459
- data-security, on page 1460
- qos-type, on page 1461
- radio-profile, on page 1461
- ssid, on page 1462
- wireless-lan country, on page 1463
- wireless-lan mgmt, on page 1463
- wlan-profile, on page 1464

passphrase

To set a Wi-Fi protected access (WPA) pass phrase, use the **passphrase** command in wireless lan profile configuration mode. To remove a pass phrase, use the **no** form on this command.

passphrase *pass-phrase*

no passphrase

Syntax Description

pass-phrase	Specifies a pass phrase to access a wireless network.

Command Default

There are no default values.

Command Modes

Wireless LAN profile configuration (config-wlan-profile)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco vManage CLI templates.

In the following example, you set a pass phrase as part of wireless configuration.

```
Device(config)# wlan-profile wl
Device(config-wlan-profile)# passphrase 0 Pass-Phrase-Sample123#
```

data-security

To configure the Wi-Fi protected access (WPA) and WPA2 data protection and network access control to use for an IEEE 802.11i wireless LAN, use the **data-security** command in wireless lan profile configuration mode. To remove security, use the **no** form of this command.

WPA authenticates individual users on the WLAN using a username and password. WPA uses the Temporal Key Integrity Protocol (TKIP), which is based on the RC4 cipher.

WPA2 implements the NIST FIPS 140-2–compliant AES encryption algorithm along with IEEE 802.1X-based authentication, to enhance user access security over WPA. WPA2 uses the Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP), which is based on the AES cipher.

Authentication is done either using preshared keys and through RADIUS authentication

data-security *security*

no data-security

Syntax Description

security Data Security Method:

Security method to apply to wireless LAN network data. It can be one of the following:

- none—No security is applied to the WLAN data. This is the default.
- wpa-enterprise—Also called WPA-802.1X mode. Enable WPA security in conjunction with a RADIUS authentication server. Configure the RADIUS server to use with the **radius-servers** command.
- wpa-personal—Also called WPA-PSK (preshared key) mode. Enable WPA security where each user enters a username and password to connect to the WLAN. Each wireless network device encrypts network traffic using a 256-bit key. Configure the password with the **wpa-personal-key** command.
- wpa/wpa2-enterprise—Enable both WPA and WPA2 security in conjunction with a RADIUS authentication server. Configure the RADIUS server to use with the **radius-servers** command.
- wpa/wpa2-personal—Enable both WPA and WPA2 security using only a username and password for authentication. Configure the password with the **wpa-personal-key** command.
- wpa2-enterprise—Enable WPA2 security in conjunction with a RADIUS authentication server. Configure the RADIUS server to use with the **radius-servers** command.
- wpa2-personal—Enable WPA2 security using only a username and password for authentication. Configure the password with the **wpa-personal-key** command.

Command Default

There are no default values.

Command Modes

Wireless LAN profile configuration (config-wlan-profile)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco vManage CLI templates.

In the following example, you a configure a security type.:

```
Device(config)# wlan-profile-sample-1
Device(config-wlan-profile)# vlan-id 100
Device(config-wlan-profile)# ssid sample-ssid-1
Device(config-wlan -profile)# data-security personal
```

qos-type

To assign a Quality of Service (QoS) profile to a WLAN, use the **qos-type** command in wireless lan profile configuration mode. To remove a qos type, use the **no** form of this command.

qos-type *profile-type*

no qos-type

Syntax Description

profile-type	Specifies a QOS profile type.

Command Default

There are no default values.

Command Modes

Wireless LAN profile configuration (config-wlan-profile)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco vManage CLI templates.

In the following example, you assign a QOS profile to a WLAN.

```
Device(config)# wlan-profile-sample-1
Device(config-wlan-profile)# vlan-id 100
Device(config-wlan-profile)# ssid sample-ssid-1
Device(config-wlan -profile)# qos-type silver
```

radio-profile

To specify the radio channel, use the **radio-profile** command in global configuration mode. To remove the radio channel, use the **no** form of this command

radio-profile *channel*

no radio-profile

Syntax Description		
	channel	Specifies a radio channel. Choose 5Ghz or 24Ghz.

Command Default There are no default values.

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco vManage CLI templates.

In the following example, you configure a 5-GHz channel and a 24-GHz channel:

```
Device(config)# radio-profile 5ghz
Device(config)# radio-profile 24ghz
```

ssid

To configure the service set identifier (SSID) for a WLAN, use the **ssid** command in wireless lan profile configuration mode. To remove an ssid, use the **no** form of this command.

Each SSID is called a virtual access point (VAP) interface. To a client, each VAP interfaces appears as a different access point (AP) with its own SSID. To provide access to different networks, assign each VAP to a different VLAN.

ssid *ssid-name*

no ssid

Syntax Description		
	ssid-name	Specify a SSID name for the WLAN.

Command Default There are no default values.

Command Modes Wireless LAN profile configuration (config-wlan-profile)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco vManage CLI templates.

In the following example, you a configure a ssid for a wireless lan:

```
Device(config)# wlan-profile wl
Device(config-wlan-profile)# ssid dev
```

wireless-lan country

To configure the wireless LAN controller's country code, use the **wireless-lan country** command in global configuration mode.

wireless-lan country *country code*

Syntax Description

country code	Specifies a two-letter or three-letter country code.

Command Default

There are no default values.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco vManage CLI templates.

In the following example, you assign a country code to the wireless LAN controller.

```
Device(config)# wireless-lan country US
```

wireless-lan mgmt

To configure details for the wireless connection on the wireless LAN controller, use the **wireless-lan mgmt** command in global configuration mode. To remove a wireless connection, use the **no** form of this command.

wireless-lan mgmt { **credential** | { **username** *username* | **password** *password* } | **ip** | { **address** *ipv4 address* } }

no wireless-lan mgmt

Syntax Description

username	Specifies the user name for the wireless LAN controller.
password	Specifies the password for the wireless LAN controller.
ipv4 address	Specifies the ip address for the wireless LAN controller.

Command Default

There are no default values.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco vManage CLI templates.

In the following example, you configure details for the wireless connection on the wireless LAN controller.

```
Device(config)# wireless-lan mgmt ip address 10.10.1.100 255.255.0.0 default-gateway
192.168.1.1
Device(config)# wireless-lan mgmt credential username admin password 0 sRe32dfst#asd
```

wlan-profile

To configure a wireless lan profile, use the **wlan-profile** command in global configuration mode. To remove a wireless lan profile, use the **no** form of this command.

wlan-profile *profile-name*

no wlan-profile

Syntax Description

profile-name	Specify a profile name used to identify the wireless profile.

Command Default

There are no default values.

Command Modes

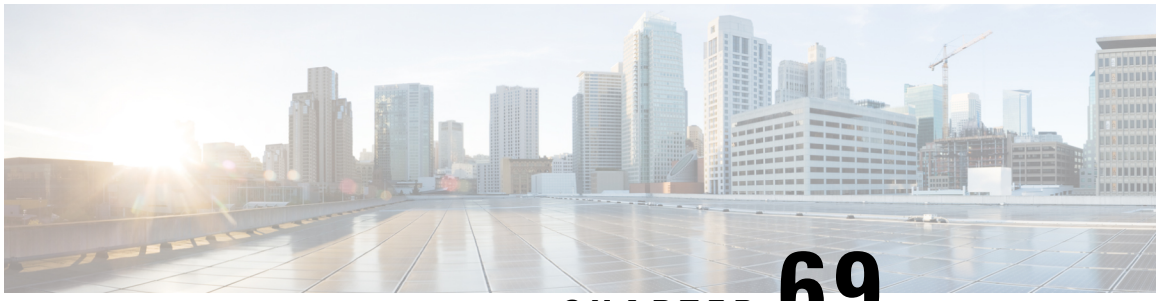
Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco vManage CLI templates.

In the following example, you configure a wireless lan profile:

```
Device(config)# wlan-profile wl
```



CHAPTER 69

Commands Qualified in Cisco IOS XE Catalyst SD-WAN Release 17.x

- Qualified CLIs for Cisco IOS XE Catalyst SD-WAN Release 17.2.1r, on page 1465
- Qualified CLIs for Cisco IOS XE Release Amsterdam 17.2.1v, on page 1467
- Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.3.1a, on page 1485
- Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.4.1a, on page 1497
- Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.5.1a, on page 1507
- Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.6.1a, on page 1514
- Qualified Commands for Cisco IOS XE Release 17.6.4, on page 1526
- Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.7.1a, on page 1526
- Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.8.1a, on page 1532
- Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.9.1a, on page 1534
- Qualified Commands for Cisco IOS XE Release 17.10.1a, on page 1535
- Qualified Commands for Cisco IOS XE Release 17.11.1a, on page 1537
- Qualified Commands for Cisco IOS XE Release 17.12.1a, on page 1541
- Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, on page 1543
- Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, on page 1544
- Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.15.1a, on page 1545
- Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.16.1a, on page 1546
- Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.18.1a, on page 1546
- Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 26.1.1 , on page 1547

Qualified CLIs for Cisco IOS XE Catalyst SD-WAN Release 17.2.1r

This section lists the CLIs that are qualified for the CLI add-on feature templates in Cisco IOS XE Catalyst SD-WAN Release 17.2.1r.

Cisco AAA Commands

```
aaa group server tacacs+ tacacs-511
server-private 172.16.0.1 key 7 110a1016141d
ip vrf forwarding 511
!
aaa authentication attempts login 5
aaa authentication login default group tacacs-511
```

```
aaa authentication enable default group tacacs-511 enable
aaa authorization config-commands
aaa authorization exec default group tacacs-511 local none
aaa authorization commands 0 default group tacacs-511 local none
aaa authorization commands 1 default group tacacs-511 local none
aaa authorization commands 2 default group tacacs-511 local none
aaa authorization commands 3 default group tacacs-511 local none
aaa authorization commands 4 default group tacacs-511 local none
aaa authorization commands 5 default group tacacs-511 local none
aaa authorization commands 6 default group tacacs-511 local none
aaa authorization commands 7 default group tacacs-511 local none
aaa authorization commands 8 default group tacacs-511 local none
aaa authorization commands 9 default group tacacs-511 local none
aaa authorization commands 10 default group tacacs-511 local none
aaa authorization commands 11 default group tacacs-511 local none
aaa authorization commands 12 default group tacacs-511 local none
aaa authorization commands 13 default group tacacs-511 local none
aaa authorization commands 14 default group tacacs-511 local none
aaa authorization commands 15 default group tacacs-511 local none
aaa authorization network default local
aaa accounting exec default start-stop group tacacs-511
aaa accounting commands 0 default start-stop group tacacs-511
aaa accounting commands 1 default start-stop group tacacs-511
aaa accounting commands 2 default start-stop group tacacs-511
aaa accounting commands 3 default start-stop group tacacs-511
aaa accounting commands 4 default start-stop group tacacs-511
aaa accounting commands 5 default start-stop group tacacs-511
aaa accounting commands 6 default start-stop group tacacs-511
aaa accounting commands 7 default start-stop group tacacs-511
aaa accounting commands 8 default start-stop group tacacs-511
aaa accounting commands 9 default start-stop group tacacs-511
aaa accounting commands 10 default start-stop group tacacs-511
aaa accounting commands 11 default start-stop group tacacs-511
aaa accounting commands 12 default start-stop group tacacs-511
aaa accounting commands 13 default start-stop group tacacs-511
aaa accounting commands 14 default start-stop group tacacs-511
aaa accounting commands 15 default start-stop group tacacs-511
aaa accounting connection default start-stop group tacacs-511
aaa accounting system default start-stop group tacacs-511
```

Cisco BGP Commands

```
router bgp 64496
neighbor 10.0.0.1 remote-as 64496
bgp graceful-restart
neighbor 10.0.0.1 ha-mode graceful-restart disable

!

router bgp 64496
address-family ipv4 unicast vrf 1
redistribute omp
redistribute static
redistribute connected

!

router bgp 64496
address-family ipv6 unicast vrf 1
redistribute omp
redistribute static
redistribute connected

!
```

```
policy-map PMap
class PMap-super-fast
priority level 1
police percent 5
class PMap-fast
priority level 2
police percent 5

class cos-map-generic
bandwidth remaining percent 5
queue-limit 108 packets
class class-default
bandwidth remaining percent 95
queue-limit 2028 packets
```

IP Commands

```
ip dns server
ip host vrf 1 test_1 192.168.0.{{variable1}}
ip host vrf 1 test_2 192.168.0.{{variable2}}
```

Privilege Exec Show Commands

```
privilege exec level 1 show logging
privilege exec level 1 show sdwan control connections
privilege exec level 1 show sdwan bfd sessions
privilege exec level 1 show sdwan system
```

Qualified CLIs for Cisco IOS XE Release Amsterdam 17.2.1v

This section lists the CLIs that are qualified for the CLI add-on feature templates in Cisco IOS XE Release Amsterdam 17.2.1v.

ACL Commands

```
ip access-list extended acl_1
 11 permit object-group employee_1 any any
!
```

AppNav Commands

```
service-insertion appnav-controller-group scg
  appnav-controller 192.3.3.1 vrf 2
  appnav-controller 192.3.3.2 vrf 2
 !
 service-insertion service-node-group acg1
  service-node 192.3.3.3
 !
 service-insertion service-context waas/1
  appnav-controller-group scg
  service-node-group      acg1
  service-policy          p1
  enable
 !
 service-insertion waas interface Tunnel2
 service-insertion waas interface Tunnel3
```

```
!
```

AppQoE Commands

```
appqoe
 no tcpopt enable
```

BFD Commands

```
bfd color mpls
  hello-interval 300000
  no pmtu-discovery
  multiplier     60
 !
 bfd color lte
  hello-interval 300000
  pmtu-discovery
  multiplier     60
 !
 bfd color 3g
  hello-interval 300000
  no pmtu-discovery
  multiplier     60
 !
 bfd app-route multiplier 6
 bfd app-route poll-interval 4294967295
```

Cisco BGP Commands

```
router bgp
  address-family no-vrf ipv4
  address-family no-vrf ipv6
  address-family with-vrf ipv4
  address-family with-vrf ipv6
  bgp always-compare-med
  bgp bestpath as-path multipath-relax
  bgp bestpath med missing-as-worst
  bgp deterministic-med
  bgp graceful-restart
  bgp bestpath compare-routerid
  bgp log-neighbor-changes
         bgp router-id

  distance bgp extern-as
  distance bgp internal-as
  distance bgp local
  maximum-paths eibgp
  timers bgp holdtime
  timers bgp keepalive-interval
 neighbor dns-address1 remote-as 999999999

  neighbor dns-address1 ebgp-multihop 255
 neighbor dns-address1 password 7 00141215174C04140B1E1E
 neighbor dns-address1 shutdown
 neighbor dns-address1 timers 65534 65535
 neighbor dns-address2 remote-as 999999
 neighbor dns-address2description test_neighbor_1
 neighbor dns-address2ebgp-multihop 255
 neighbor dns-address2 password 7 13151601181B0B382F1B7A
 neighbor dns-address2 shutdown
 neighbor dns-address2 timers 65534 65535
```

```
 neighbor 10.228.0.129 remote-as 999999999
 neighbor 10.228.0.129 advertise-map ADVERTISE non-exist-map NON-EXIST
 neighbor 10.228.0.129 ha-mode graceful-restart disable
  propagate-aspath
  address-family ipv4 unicast vrf 1
  redistribute connected
  redistribute omp
  redistribute static
  exit-address-family
 !
 address-family ipv6 unicast vrf 1
  redistribute connected
  redistribute omp
  redistribute static
  exit-address-family
          propagate-aspath
 !
 address-family ipv4 unicast
  aggregate-address 192.168.51.0 255.255.255.0 as-set summary-only
  aggregate-address 192.168.52.0 255.255.255.0 as-set summary-only
  neighbor 10.0.0.1 advertise-map ADVERTISE non-exist-map NON-EXIST
  neighbor dns-address1 remote-as 999999999
  neighbor dns-address1 activate
  neighbor dns-address1 advertisement-interval 600
  neighbor dns-address1 maximum-prefix 2147483647 100
  neighbor dns-address1 maximum-prefix 769434 100 restart 65535
  neighbor dns-address1 next-hop-self
  neighbor dns-address1 send-community both
  neighbor dns-address2 remote-as 999999
  neighbor dns-address2 activate
  neighbor dns-address2 advertisement-interval 600
  neighbor dns-address2 maximum-prefix 98765 100 restart 65535
  neighbor dns-address2 next-hop-self
  neighbor dns-address2 route-map <route_map_name>
  neighbor dns-address2 send-community both
  neighbor dns-address2 timers 3 9
  network dns-address2  mask 255.255.255.0
  network 192.168.51.0 mask 255.255.255.0
  network 192.168.52.0 mask 255.255.255.0
  exit-address-family
 !
 timers bgp 60 180
!
```

Class Map Commands

```
class-map match-any BestEffort
  match qos-group 3
 !
 class-map match-any Bulk
  match qos-group 4
 !
 class-map match-any Critical
  match qos-group 1
 !
 class-map match-any Critical-Low
  match qos-group 2
 !
 class-map match-any BULK
  match qos-group 2
 !
 class-map match-any CONTROL-SIGNALING
  match qos-group 4
 !
```

```
class-map match-any CRITICAL-DATA
 match qos-group 1
!
class-map match-any Default
 match qos-group 5
!
class-map match-any INTERACTIVE-VIDEO
 match qos-group 3
!
class-map match-any LLQ
 match qos-group 0
!
class-map match-any Queue0
 match qos-group 0
!
class-map match-any Queue1
 match qos-group 1
!
class-map match-any Queue2
 match qos-group 2
!
class-map match-any Queue3
 match qos-group 3
!
class-map match-any Queue4
 match qos-group 4
!
class-map match-any Queue5
 match qos-group 5
!
class-map type inspect match-all cmap
 match access-group name cmap
!
   pass
 !
class-map match-any Queue4
 match qos-group 0
!
```

Crypto Commands

```
crypto ikev2 authorization policy li_policy
 exit
 no crypto ikev2 diagnose error
 crypto ikev2 keyring if-ipsec256-ikev2-keyring
  peer if-ipsec256-ikev2-keyring-peer
   address 172.16.93.1
   pre-shared-key cisco123
  !
 !
 crypto ikev2 policy policy1-global
  proposal p1-global
 !
 crypto ikev2 profile if-ipsec256-ikev2-profile
  aaa authorization group psk list default li_policy
  authentication local pre-share
  authentication remote pre-share
  no config-exchange request
  keyring local if-ipsec256-ikev2-keyring
  lifetime 86400
  match identity remote address 172.16.93.2
 !
 crypto ikev2 proposal p1-global
```

```
 encryption aes-cbc-128 aes-cbc-256
 group 14 15 16 2
 integrity sha1 sha256 sha384 sha512
!
!
crypto ipsec transform-set if-ipsec256-ikev2-transform esp-gcm 256
 mode tunnel
!
crypto ipsec profile if-ipsec256-ipsec-profile
 set ikev2-profile if-ipsec256-ikev2-profile
 set pfs group16
 set transform-set if-ipsec256-ikev2-transform
 set security-association lifetime kilobytes disable
 set security-association lifetime seconds 3600
 set security-association replay window-size 512
!
no crypto isakmp diagnose error
       crypto isakmp aggressive-mode disable
parameter-map type inspect-global
 multi-tenancy
 vpn zone security
!
no crypto ikev2 diagnose error
no crypto isakmp diagnose error
```

EIGRP Commands

```
router eigrp eigrp-name
 address-family ipv4 vrf {{SVPN}} autonomous-system {{SVPN}}
af-interface {{LAN_EIGRP_INT1_name}}
 no dampening-change
 no dampening-interval
 hello-interval 5
 hold-time      15
 split-horizon
 exit-af-interface
!
 af-interface {{LAN_EIGRP_INT2_name}}
  no dampening-change
  no dampening-interval
  hello-interval 5
  hold-time      15
  split-horizon
  exit-af-interface
 !
{{LAN_EIGRP_neighbor1_tf}}  neighbor {{LAN_EIGRP_neighbor1_ip_addr}}
{{LAN_EIGRP_neighbor1_src_int}}
{{LAN_EIGRP_neighbor2_tf}}  neighbor {{LAN_EIGRP_neighbor2_ip_addr}}
{{LAN_EIGRP_neighbor2_src_int}}
{{LAN_EIGRP_neighbor3_tf}}  neighbor {{LAN_EIGRP_neighbor3_ip_addr}}
{{LAN_EIGRP_neighbor3_src_int}}
{{LAN_EIGRP_neighbor4_tf}}  neighbor {{LAN_EIGRP_neighbor4_ip_addr}}
{{LAN_EIGRP_neighbor4_src_int}}
{{LAN_EIGRP_neighbor5_tf}}  neighbor {{LAN_EIGRP_neighbor5_ip_addr}}
{{LAN_EIGRP_neighbor5_src_int}}
network {{LAN_EIGRP_INT1_linknet}}
 network {{LAN_EIGRP_INT2_linknet}}
  topology base
   redistribute omp metric 1000000 255 1 1500
   redistribute static
   exit-af-topology
  !
  exit-address-family
```

```
 !
!
```

Global Configuration Commands

```
memory free low-watermark processor 70694
         platform punt-keepalive disable-kernel-core
 no service pad
 no service tcp-small-servers
 no service udp-small-servers
 platform console virtual
 platform qfp utilization monitor load 80
 platform punt-keepalive disable-kernel-core
 hostname myorg
 username admin privilege 15 secret
 username
 username employee1 privilege
 username employee1 secret encryption
 username employee1 secret secret
 clock timezone UTC
 logging monitor
 logging persistent
 logging persistent size 104857600 filesize 10485760
 logging buffered
 logging console
 logging trap errors
 logging rate-limit
 logging host 10.90.9.6 vrf 4
 logging source-interface loopback111 vrf 4
 login on-success log
 no crypto ikev2 diagnose error
 no crypto isakmp diagnose error
 crypto pki trustpoint TP-self-signed-3865005142
  enrollment selfsigned
  revocation-check none
  subject-name     cn=IOS-Self-Signed-Certificate-3865005142
 line con 0
  login authentication default
  speed    9600
  stopbits 1
 !
  login authentication default
  speed    19200
  stopbits 1
 line vty 0 4
  transport input ssh
 line vty 5 80
  transport input ssh
 !mac address-table aging-time <timeout>

 lldp run
```

Interface GigabitEthernet Commands

```
 no shutdown
  arp timeout
  ip address 192.10.6.5
         vrf forwarding vrf10
         ip address dhcp client-id GigabitEthernet1
  no ip redirects
  ip mtu
  mtu
```

```
  ip nat outside
  ip ospf 65535 area 1
  ip ospf authentication message-digest
  ip ospf network     broadcast
  ip ospf cost
  ip ospf dead-interval
  ip ospf hello-interval
  ip ospf message-digest-key 255 md5 7 00051105005E0D01072846
  ip ospf priority
  ip ospf retransmit-interval
  negotiation auto
  service-policy output  policy_1
         ip tcp adjust-mss 1100
         cdp enable
         ip nat outside
         bandwidth 100000
 vrrp 64 address-family ipv4
   vrrpv2
   track 2 shutdown
   address 10.50.4.3 primary
   priority 11
   timers advertise 1000


interface GigabitEthernet1.101
  no shutdown
  encapsulation dot1Q 101
  vrf forwarding 2
  ip address 192.168.66.1
  no ip redirects
         ip directed-broadcast
  ip mtu    1496
  ipv6 address 2001:DB8::1
  ipv6 enable
  ip nbar protocol-discovery
         ip policy route-map policy_1
         ip helper-address 10.8.4.5
         ip helper-address 10.50.4.6

 tunnel-interface
    encapsulation gre weight 1
           encapsulation ipsec weight 1
    no border
    color lte
    no last-resort-circuit
    no low-bandwidth-link
    max-control-connections       1
    exclude-controller-group-list 1
    no vbond-as-stun-server
    vmanage-connection-preference 5
    port-hop
    carrier                       default
    nat-refresh-interval          5
    hello-interval                1000
    hello-tolerance               12
    no allow-service all
    no allow-service bgp
    allow-service dhcp
    allow-service dns
    allow-service icmp
    no allow-service sshd
    no allow-service netconf
    no allow-service ntp
    no allow-service ospf
    no allow-service stun
```

```
    allow-service https
    no allow-service snmp
 bandwidth-downstream 300000000

 interface GigabitEthernet4.302
   tloc-extension GigabitEthernet
   access-list 4451-Marking-Spoke in

interface Dialer1
  no shutdown
  encapsulation ppp
  ip address negotiated
  ip nat outside
  dialer pool 1
  ppp chap hostname ntt
  ppp chap password ntt
  ppp authentication chap calling

interface Loopback100
 interface VirtualPortGroup0
 interface Vlan1

pppoe enable group global
pppoe-client dial-pool-number

interface Tunnel
 ip unnumbered GigabitEthernet0/2.101
  no ip redirects
  ipv6 unnumbered GigabitEthernet0/2.101
  no ipv6 redirects
  tunnel source GigabitEthernet0/2.101
  tunnel mode sdwan



interface atm 0/3/0
description site1
ip mtu 1496
no shutdown

interface atm 0/3/0.1 point-to-point
description site1
ip mtu 1496
[no] ip address 10.0.0.0 255.255.255.252
no shutdown
load-interval 30
pvc 0/100
  [no] shutdown
  bridge-dot1q encap 1
  encapsulation aal5snap
  dialer pool-member 1
  protocol ppp dialer


interface GigabitEthernet1
description branch1
no ip address
no shutdown
ip mtu 1500

interface GigabitEthernet4.302
description branch1
encapsulation dot1Q 101
pppoe enable group global
pppoe-client dial-pool-number
```

```
no shutdown
[no] ip address 192.10.6.5
ip mtu 1496

interface Dialer1
ip address negotiated
encapsulation ppp
dialer pool 1
dialer-group 1
ppp authentication chap callin
ppp chap hostname ntt
ppp chap password ntt
ppp pap sent-username ntt password ntt
ppp sent-password ntt password 0 ntt
no shutdown

controller VDSL 0/3/0
description branch1
operating mode auto
[no] firmware filename bootflash:firmware
[no] modem auto
[no] sra
no shutdown
training log filename flash:4431.log
[no] bitswap
line-mode single-wire line 0
sync mode none
no diagnostics DELT
```

IP Commands

```
ip dhcp use hardware-address client-id
 no ip dhcp use class
         ip host <vbond ip_address1 ip_address2>
 ip ssh version 2
 ip dhcp use vrf remote
 ip multicast route-limit
 ip route
 ip name-server 10.70.1.2
 ip name-server vrf
         ip prefix-list prfx1  permit 172.16.55.1
 ip bootp server
 no ip source-route
 no ip http server
         ip route vrf Mgmt-intf 172.16.55.10
         ipv6 route vrf Mgmt-intf 2001:DB8:101::1
         ip tcp mss 1200
 no ip http secure-server
 no ip igmp ssm-map query dns
 ip nat settings central-policy
 ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet5 overload
 ip nat translation tcp-timeout
 ip nat translation udp-timeout
 cdp run
 object-group service cdp-service-1
  ip
 ip access-list extended access_list_1
    permit object-group group1 any any
 ip arp proxy disable
 no ip rcmd rcp-enable
 no ip rcmd rsh-enable
 no ip domain lookup
         ip dhcp use class
```

```
 ip dhcp pool vrf-1-GigabitEthernet5
  option 150 ip ip-list
  vrf
  lease 365 0 0
  default-router 10.1.19.15
  dns-server 172.16.79.1
  domain-name dns1
  network 255.255.255.0
 ip http authentication local
 no ip finger
 ip http server
 ip http secure-server
 no ip igmp ssm-map query dns

 ip nat pool natpool-GigabitEthernet0/0/0-0 10.4.1.11 10.4.1.250 prefix-length 24
 ip nat inside source list global-list pool natpool-GigabitEthernet0/0/0-0 overload
egress-interface GigabitEthernet4
 ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet4.101
overload
 ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet4.102
overload
 ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet4.103
overload
 ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet4.104
overload
 ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet4.105
overload
 ip nat translation tcp-timeout 10
 ip nat translation udp-timeout 40
 ip nat route vrf 65529 0.0.0.0 0.0.0.0 global
 ip nat route vrf 2 172.16.200.0 255.255.255.0 global
 ipv6 route vrf 1 2001:DB8:EF::1
 vlan internal allocation policy ascending
 ip redirects
 route-map trigger permit
 match ip address prefix
 line vty 0 4
 access-class
 ipv6 access-class
```

Logging Commands

```
logging trap informational syslog-format rfc5424
logging tls-profile profile1 tls-version TLSv1.1
logging tls-profile profile1 ciphersuite aes-256-cbc-sha
```

NAT Commands

```
nat64 translation timeout tcp 60
nat64 translation timeout udp 1
```

NTP Commands

```
ntp authentication-key 65535 md5 test
 ntp server 10.0.1.1 source GigabitEthernet8 key 65535 prefer version 4
 ntp source GigabitEthernet8
 ntp trusted-key
 ntp access-group peer 25
```

Object Group Commands

```
object-group network Auth-Servers
  host 10.16.137.22
  !
 object-group service ZBF-DIA-External
 tcp 80
 udp
 tcp range 1024 65535
 tcp source 23
 ip
 icmp
 !
```

OMP Commands

```
omp
   no shutdown
   overlay-as       4294967295
   send-path-limit  16
   ecmp-limit       16
   graceful-restart
   no as-dot-notation
   timers
    holdtime               65535
    advertisement-interval 65535
    graceful-restart-timer 43200
    eor-timer              3600
   exit
   address-family ipv4
    advertise bgp
    advertise ospf external
    advertise connected
    advertise static
    advertise eigrp
    advertise lisp
    advertise isis
   !
   address-family ipv6
    advertise bgp
    advertise connected
    advertise static
    advertise eigrp
    advertise lisp
    advertise isis
```

OSPF Commands

```
router ospf 1 10
  auto-cost reference-bandwidth 100
  timers throttle spf 200 1000 10000
  router-id 10.68.202.1
  compatible rfc1583
          default-information originate
          default-information originate metric-type 1
  distance ospf external 110
  distance ospf inter-area 110
  distance ospf intra-area 110
  redistribute connected subnets
 redistribute nat-route dia
 !
 max-metric router-lsa on-startup 86400
  area 4294967295 nssa no-summary
  area 4294967295 range 10.1.1.0 255.255.255.0 not-advertise
```

```
  area 4294967295 range 192.168.1.0 255.255.255.0 cost 16777214
  area 4294967295 range 172.16.5.0 255.255.255.0 advertise
 default-information originate always metric 16777214 metric-type 1
 redistribute static
```

Policy Commands

```
route-map rmap1 deny 10
  match ip address prefix-list prfx1
 !
 route-map rmap1 permit 10
  match as-path 120
  match ip address prefix-list prfx1 !
 route-map clear-df permit 10
 !

parameter-map type inspect-global
  alert on
  log dropped-packets
  multi-tenancy
  vpn zone security
 !

policy
  app-visibility
  flow-visibility
  implicit-acl-logging
  log-frequency        1000
 policer pol1
 rate 500000000
burst 15000
exceed drop
  lists
   data-prefix-list Email-Server
    ip-prefix prfx1



class-map
   class LLQ queue 0
   class Queue0 queue 0
   class VOICE queue 0
   class CRITICAL-DATA queue 1
   class Queue1 queue 1
   class BULK queue 2
   class Queue2 queue 2
   class INTERACTIVE-VIDEO queue 3
   class Queue3 queue 3
   class CONTROL-SIGNALING queue 4
   class Queue4 queue 4
   class Default queue 5
   class Queue5 queue 5
  !
   rewrite-rule Branch-QoS-Rewrite-Template
   class BULK low dscp 10
   class BULK high dscp 10
   class CRITICAL-DATA low dscp 28
   class CRITICAL-DATA high dscp 28
   class INTERACTIVE-VIDEO low dscp 34
   class INTERACTIVE-VIDEO high dscp 34
  !
   access-list acl1
   sequence 10
```

```
    match
     destination-ip 172.16.5.10
    !
    action drop
   default-action accept
    action drop
     count 192-167-199-DROP-CNT
  access-list 4451-Marking-Spoke
   sequence 1
    match
     destination-ip 172.16.10.5
    !
    action accept
     count SSL
     class LLQ
     count EXCHANGE
     class CONTROL-SIGNALING
    action accept
     count RTP
     class LLQ
    action accept
     count HTTP_10K_60K
     class BULK
     action accept
     count HTTP_BROWSING
     class BULK
     count Oracle
     class CRITICAL-DATA
     count Citrix
     class INTERACTIVE-VIDEO
     count SSL
     class BULK
     count EXCHANGE
     class CONTROL-SIGNALING
     count Video
     class INTERACTIVE-VIDEO

"access-list Marking-HQ
   sequence 1
    match
     source-ip 10.74.201.203/32"
 "!
   sequence 21
    match
     source-ip 10.74.201.202/32
    !
    action accept
     set
      dscp 18"
 "policy-map type inspect security-zbfw
    class security-zbfw-seq-1
     inspect"
 "sequence 181
     match
      destination-data-prefix-list QOS-QUALYS-SCANNERS"
 "sequence 11
     match
      destination-ip   10.53.128.23/32
      destination-port 443"
```

Policy Map Commands

```
policy-map type inspect pmap1
 class cos-map-generic inspect
```

```
 bandwidth remaining percent 5
 policy-map Branch-QoS-Policy
  class Queue0
   priority level 1
   police rate percent 30
   !
  !
  class Queue1
   bandwidth remaining ratio 20
   random-detect precedence-based
  !
  class class-default
   bandwidth remaining ratio 10
   random-detect precedence-based
  !
  class Queue3
   bandwidth remaining ratio 20
   random-detect precedence-based
  !
  class Queue4
   bandwidth remaining ratio 10
   random-detect precedence-based
  !
  class Queue5
   bandwidth remaining ratio 10
   random-detect precedence-based
  !
 !
 policy-map shape_GigabitEthernet0/0/1
  class class-default
   service-policy Branch-QoS-Policy
   shape average 1000000000
  !
  class class-default
    drop
  !
 !
```

QOS Policy commands

```
policy-map QOS-POLICY-MAP
 class Queue0
  priority percent 30
 class Queue1
  bandwidth percent 20
 class Queue3
  bandwidth percent 20
 class class-default
  bandwidth percent 30
```

```
policy-map QOS-POLICY-MAP
 class Queue0
  priority percent 30
 class Queue1
  bandwidth percent 20
  random-detect
 class Queue3
  bandwidth percent 20
 class class-default
  bandwidth percent 30
  random-detect
```

```
policy-map QOS-POLICY-MAP
 class Queue0
```

```
  priority percent 30
 class Queue1
  bandwidth percent 20
  random-detect
 class Queue3
  bandwidth percent 20
 class class-default
  bandwidth percent 30
  random-detect

policy-map QOS-POLICY-MAP
 class Queue0
  priority level 1
  police rate percent 30
 class Queue1
  bandwidth percent 20
  random-detect
 class Queue3
  bandwidth percent 20
 class class-default
  bandwidth percent 30
  random-detect

policy-map QOS-POLICY-MAP
 class Queue0
  priority level 1
  police rate percent 30
 class Queue1
  bandwidth remaining ratio 20
  random-detect
 class Queue3
  bandwidth remaining ratio 20
 class class-default
  bandwidth remaining ratio 30
  random-detect
```

RADIUS Commands

```
radius-server dead-criteria time 10 tries 3
radius-server deadtime 15
```

Security Commands

```
security
  ipsec
   rekey               1209600
   replay-window       4096
   authentication-type sha1-hmac ah-sha1-hmac ah-no-id
   pairwise-keying
```

SNMP Commands

```
snmp-server community Log view Logging RO
 snmp-server community Trap view Interface RO
 snmp-server contact
 snmp-server enable traps
 snmp-server engineID local
 snmp-server group test_group_v3 v3 noauth read view_test_v3
 snmp-server host 10.100.51.1 vrf 1 version 2c Log udp-port 7081
 snmp-server host 10.1.15.15 version 3 noauth test_user_v3 udp-port 161
 snmp-server community xxxxx view yyyyy RO acl-name1
 snmp-server ifindex persist
 snmp-server location
```

```
 snmp-server trap timeout
 snmp-server trap-source Loopback

 snmp-server user test_user_v3 test_group_v3 v3 encrypted
 snmp-server view Interface 1.3.1 included
 snmp-server view Logging 1.4.1 included
 snmp-server view view_test_v3 1.3.6.1 included
```

SSL Proxy Commands

```
sslproxy
  no enable
  rsa-key-modulus      2048
  certificate-lifetime 730
  eckey-type           P256
  ca-tp-label
  settings expired-certificate  drop
  settings untrusted-certificate drop
  settings unknown-status       drop
  settings certificate-revocation-check none
  settings unsupported-protocol-versions drop
  settings unsupported-cipher-suites drop
  settings failure-mode         close
  settings minimum-tls-ver      TLSv1
 no tcpproxy enable
```

System Commands

```
  gps-location latitude 37.368140
  gps-location longitude -121.913658
  system-ip
  overlay-id
  site-id
  port-offset
  control-session-pps
         controller-group-list 1 2
         device-groups  a
  admin-tech-on-failure
  sp-organization-name
  organization-name
         max-omp-sessions      8
  port-hop
  track-transport
  track-default-gateway
  upgrade-confirm
  console-baud-rate
  vbond 192.168.5.4 port 12346
 logging
enable
```

UTD Commands

```
utd multi-tenancy
 utd engine standard multi-tenancy
  utd global
   file-reputation
    cloud-server   cloud-isr-asn.amp.cisco.com
    est-server     cloud-isr-est.amp.cisco.com
    query-interval 300
   !
   file-analysis
    cloud-server panacea.threatgrid.com
```

```
  !
 !
 file-analysis profile FILE-ANA-PROFILE1
  file-types
   pdf
   ms-exe
   new-office
   rtf
   mdb
   mscab
   msole2
   wri
   xlw
   flv
   swf
  !
  alert level critical
 !
 file-reputation profile FILE-REP-PROFILE1
  alert level critical
 !
 file-inspection profile FILE-INS-PROFILE1
  analysis profile FILE-ANA-PROFILE1
  reputation profile FILE-REP-PROFILE1
!
```

Voice Commands

```
sip-ua
 !
 voice class codec 1000
  codec preference 1 g729r8
  codec preference 2 g711ulaw bytes 160
  codec preference 3 g711alaw bytes 160
  codec preference 4 g722-64 bytes 160
 !
 voice service voip

  allow-connections sip to sip
  no supplementary-service sip handle-replaces
  no supplementary-service sip moved-temporarily
  no supplementary-service sip refer
  sip
   registrar server expires max 300 min 200
  !
 !
 voice register global
  max-dn   200
  max-pool 100
  system message "SRST mode"
 !
 voice register pool 100
  id network 10.0.0.0 mask 255.0.0.0
 !
 dial-peer voice 1000 voip
  description         Branch 1

  destination-pattern 1T
  no shutdown
  voice-class codec 1000
  session transport udp
  session protocol sipv2
  session target ipv4:10.1.101.8
  dtmf-relay rtp-nte digit-drop sip-kpml sip-notify
```

```
!
dial-peer voice 2000 voip
 description         Branch 1
  destination-pattern 2T
 no shutdown
 voice-class codec 1000
 session transport udp
 session protocol sipv2
 session target ipv4:10.1.101.8
 dtmf-relay rtp-nte digit-drop sip-kpml sip-notify
!
dial-peer voice 8000 voip
 description         Branch 7
  destination-pattern 8T
 no shutdown
 voice-class codec 1000
 session transport udp
 session protocol sipv2
 session target ipv4:10.1.101.8
 dtmf-relay rtp-nte digit-drop sip-kpml sip-notify
!
dial-peer voice 9000 voip
 description         CallManager for Dial 9

 destination-pattern 9T
 no shutdown
 voice-class codec 1000
 session transport udp
 session protocol sipv2
 session target ipv4:10.1.101.8
 dtmf-relay rtp-nte digit-drop sip-kpml sip-notify
!
```

VRF Commands

```
vrf definition
   address-family ipv4
   address-family ipv6
   description
   rd
   route-target export
   route-target import
 service tcp-keepalives-in
 service tcp-keepalives-out
 service tcp-small-servers
 service udp-small-servers
```

Zone Based Firewall commands

```
zone security LAN
  vpn 2
 !
 zone security WAN
  vpn 0
 !
 zone-pair security ZP_LAN_WAN_test-policy source LAN destination WAN
  service-policy type inspect test-policy
 !
 zone-pair security ZP_WAN_LAN_test-policy source WAN destination LAN
  service-policy type inspect test-policy
```

Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.3.1a

Table 119: Feature History

Feature Name	Release Information	Description
Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a Cisco vManage Release 20.3.1	Starting Cisco IOS XE Catalyst SD-WAN Release 17.3.1a, you can use additional commands in CLI Add-on feature templates.

AAA Commands

- `aaa authentication password-prompt <>`
- `aaa authentication username-prompt <>`
- `aaa authentication login default group tacacs+ local`
- `aaa authentication enable default group tacacs+ enable`
- `aaa authorization console`
- `aaa authorization config-commands`
- `aaa authorization exec default local group tacacs+`
- `aaa authorization commands 15 default local group tacacs+`
- `aaa accounting connection default stop-only group tacacs+`
- `aaa accounting exec default start-stop group tacacs+`
- `aaa accounting commands 15 default start-stop group tacacs+`
- `aaa authorization network default local`
- `aaa accounting system default start-stop group tacacs+`
- `aaa authentication attempts login`
- `aaa authentication ppp dialinppp local`
- `login block-for <> attempts <> within`
- `login quiet-mode access-class <ACL>`
- `tacacs server server name`
- ```
  tacacs server server name
  address ipv4 192.0.2.1
  ```
- `ip tacacs source-interface Loopback0`
- ```
  tacacs server server-name
  key Ys6WhgHS40
  ```

ACL Commands

- ip access-list standard <>
- ip access-list standard 15
  permit <>
- ip access-list standard 15
  deny <>
- ip access-list standard 15
  deny any <>
- ip access-list extended <>
- ip access-list extended 105
  <> ip any any
- ip access-list extended 105
  deny <> any any
- ip access-list extended 105
  deny ip <> any
- ip access-list extended 105
  deny ip any <>
- ip access-list extended EXTACL
  deny ip any any <>
- ip access-list extended DSCP-OUT-SAA
  <> udp any range 64001 64005 any
- ip access-list extended DSCP-OUT-SAA
  permit <> any range 64001 64005 any
- ip access-list extended DSCP-OUT-SAA
  permit udp <> range 64001 64005 any
- ip access-list extended DSCP-OUT-SAA
  permit udp any range <> 64005 any
- ip access-list extended DSCP-OUT-SAA
  permit udp any range 64001 <> any
- ip access-list extended BGP-D1
  permit tcp any eq <> any
- ip access-list extended DSCP-OUT-SAA
  permit udp any range 64001 64005 <>
- ip access-list extended DSCP-OUT-SAA
  permit icmp host <> any
- ip access-list extended DSCP-OUT-SAA
  permit udp any any range <> 64005
- ip access-list extended DSCP-OUT-SAA
  permit udp any any range 64001 <>
- ip access-list extended DSCP-OUT-SAA
  permit udp any range 64001 64005 any <>
- ip access-list extended BGP-D1
  permit tcp any any eq <>

ATM Commands

- interface ATM <>
- interface ATM 0/0/0
  ip <>
- interface ATM 0/0/0
  atm <>
- interface ATM 0/0/0
  <>
- interface ATM 0/2/0.1 <>
- interface ATM 0/2/0.1 point-to-point
  pvc 0/1
  encapsulation aal5mux <>
- interface ATM 0/2/0.1 point-to-point
  pvc 0/1
  encapsulation <>
- interface ATM 0/2/0.1 point-to-point
  pvc 0/1
  vbr-nrt <> 48 1
- interface ATM 0/2/0.1 point-to-point
  pvc 0/1
  vbr-nrt 48 <> 1
- interface ATM 0/2/0.1 point-to-point
  service-policy output <>
- interface ATM 0/2/0.1 point-to-point
  <>
- interface ATM 0/2/0.1 point-to-point
  pvc 0/1
  oam-pvc <>
- interface ATM 0/2/0.1 point-to-point
  pvc 0/1
  oam-pvc manage <>
- interface ATM 0/2/0.1 point-to-point
  pvc 0/1
  oam retry <>

Frame Relay Commands

- interface Serial 0/1/0
  encapsulation frame-relay <ietf>
- interface Serial 0/1/0
  frame-relay lmi-type <ansi>
- interface Serial 0/1/0
  frame-relay intf-type <dte>
- interface Serial 0/1/0
  frame-relay intf-type <dce>

- interface Serial 0/1/0
  frame-relay interface-dlci <>
- interface Serial 0/1/0
  < >
- interface Serial 0/1/0.2 point-to-point
  ip address <192.0.2.1> 255.255.255.0
- interface Serial 0/1/0.2 point-to-point
  frame-relay interface-dlci <>
- interface Serial 0/1/0.2 point-to-point
  <>
- interface Serial 0/0/1:5
  ip address <192.0.2.1> 255.255.255.0
- interface Serial 0/0/1:5
  encapsulation frame-relay
- interface Serial 0/0/1:5
  frame-relay intf-type <dte>
- interface Serial 0/0/1:5
  frame-relay intf-type <dce>
- interface Serial 0/0/1:5
  <>
- interface MFR<>
- interface MFR 1
  ip address <192.0.2.1> 255.255.255.0
- interface MFR 1
  frame-relay multilink bandwidth-class <a>
- interface MFR 1
  frame-relay multilink bandwidth-class <b>
- interface MFR 1
  frame-relay multilink bandwidth-class c <>
- interface MFR 1
  frame-relay intf-type <dte>
- interface MFR 1
  frame-relay intf-type <dce>
- interface MFR 1
  frame-relay interface-dlci <>
- interface MFR 1
  <>

HTTP Commands

- no ip http server
- no ip http secure-server

Interface Commands

- configure interface <id> mtu <size>
- configure interface <id> mtu <size greater than 1500 and upto 9000>
- configure interface <id> ip mtu <size>
- configure interface <id> description
- configure interface <id> hold-queue in
- configure interface <id> hold-queue out
- configure interface <id> no shutdown
- configure interface ATM <id> encapsulation dot1Q <vlan-id>
- configure interface Ethernet <id> encapsulation dot1Q <vlan-id>

IP Commands

- interface GigabitEthernet2.1
  encapsulation dot1Q 1
  ip address <> 255.255.255.0
- interface GigabitEthernet 3
  ip address <> 255.255.255.0
- interface ATM0/3/0
  ip address <> 255.255.255.0
- interface ATM0/3/0.1
  ip address <> 255.255.255.0
- interface Serial2/0
  ip address <> 255.255.255.0
- interface Loopback 2
  ip address <> 255.255.255.0
- interface Dialer2
  ip address <> 255.255.255.0
- interface Vlan 1
  ip address <> 255.255.255.0
- interface Dialer 2
  ip unnumbered <>
- ip route 192.0.2.1 255.255.255.0 198.51.100.1 track <>
- ip route 192.0.2.1 255.255.255.0 Dialer2 198.51.100.1 tag <>
- ip route 192.0.2.1 255.255.255.0 198.51.100.1 tag <>
- ip route 192.0.2.1 255.255.255.0 Dialer2 tag <>
- ip route 192.0.2.1 255.255.255.0 Dialer2 198.51.100.1 <>
- ip route 192.0.2.1 255.255.255.0 198.51.100.1 <>
- ip route 192.0.2.1 255.255.255.0 Dialer2 <>

- ip route 192.0.2.1 255.255.255.0 GigabitEthernet2 <>
- ip route 192.0.2.1 255.255.255.0 <>
- ip route vrf 1 192.0.2.1 255.255.255.0 198.51.100.1 track <>
- ip route vrf 1 192.0.2.1 255.255.255.0 198.51.100.1 tag <>
- ip route vrf 1 192.0.2.1 255.255.255.0 198.51.100.1 <>
- ip route vrf 1 192.0.2.1 255.255.255.0 GigabitEthernet2 <>
- ip route vrf 1 192.0.2.1 255.255.255.0 <>
- ip icmp rate-limit unreachable <>
- interface Dialer 2
  ip <>
- interface GigabitEthernet 2.100
  ip <>
- interface GigabitEthernet 2
  ip <>
- ip <>
- ip icmp redirect <host>
- ip icmp redirect <subnet>
- interface Tunnel 10
  ip <>
- ip ftp <>
- ip rcmd <>
- interface Dialer 2
  ip address <>
- interface GigabitEthernet 2
  ip address <>
- interface Virtual-Template 2
  ip address <>

IPoE MTU

- mtu<size>
- ip mtu <size>

IPv6 Commands

- no ipv6 source-route
- interface GigabitEthernet 2
  ipv6 <>
- interface GigabitEthernet 2.100
  ipv6 <>

- interface GigabitEthernet 2
  ipv6 nd ra suppress <>
- interface GigabitEthernet 2
  ipv6 nd prefix <>
- interface GigabitEthernet 2
  ipv6 nd router-preference <>
- interface GigabitEthernet 2
  ipv6 address autoconfig
- interface GigabitEthernet 2
  ipv6 nd other-config-flag

Line Commands

- line console 0
  transport <>
- line vty 0 4
  transport <>
- line console 0
  transport output <ssh>
- line vty 0 4
  transport output <ssh>

Logging Commands

- logging console <>
- logging monitor <>
- logging <>
- banner login <>

PPP Commands

- interface Dialer 1
  encapsulation ppp
- interface Dialer 2
  encapsulation ppp
  ppp authentication chap <>
- interface Dialer 3
  encapsulation ppp
  ppp chap hostname <>
- interface Dialer 4
  encapsulation ppp
  ppp chap password 0 <>
- interface ATM 0/3/0
  pvc 0/1
  encapsulation aal5mux ppp <>

- interface ATM 0/3/0.1 point-to-point
  pvc 0/20
   encapsulation aal5mux ppp <>
- interface ATM 0/3/0
   pvc 0/1
   encapsulation aal5mux ppp Virtual-Template <>

PPPoEoVlan - Chap Commands

- policy-map COS-OUT-SHAPED
- class class-default
- set cos {dot1P_Value}
- interface {Ethernet_Interface}
- mtu 1774
- no ip address
- no shutdown pppoe enable group global
- pppoe-client dial-pool-number 1
- pppoe-client ppp-max-payload 1766
- service-policy output COS-OUT-SHAPED
- no shutdown
- interface Dialer1
- mtu 1766
- ip unnumbered Loopback0
- encapsulation ppp
- dialer pool 1
- ppp authentication chap callin
- ppp chap hostname {Usename}
- ppp chap password {Chap_Password}
- no shutdown

Routemap Commands

- route-map <>
- route-map abc <permit> 10
- route-map def <deny> 20
- route-map abc permit <>
- route-map map-tag deny <>

- route-map map-tag permit 25
  match length <> 2147483647
- route-map map-tag permit 30
  match length 1 <>
- route-map map-tag permit 35
  match ipv6 address prefix-list <>
- route-map map-tag permit 40
  match ipv6 address <>
- route-map map-tag permit 311
  set ipv6 next-hop <2::2>
- route-map map-tag permit 45
  set ipv6 precedence <>
- route-map map-tag permit 50
  set interface Dialer <1>
- route-map map-tag permit 55
  set interface GigabitEthernet <3>
- route-map map-tag permit 60
  set interface Tunnel <1>
- route-map map-tag permit 251
  set ipv6 default next-hop <1::1>
- route-map map-tag permit 56
  set default interface GigabitEthernet <3>
- route-map map-tag permit 79
  set default interface Tunnel <11>
- route-map map-tag permit 75
  set vrf <1>
- interface GigabitEthernet 3
  ipv6 policy route-map <>
- ipv6 local policy route-map <>

Security Commands

To configure posture assessment use the CLI Add-on template in Cisco vManage.

Configure IEEE 802.1x authentication and authorization

```
policy-map type control subscriber simple_dot1x
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x
!
interface GigabitEthernet0/1/7
 switchport access vlan 22
 switchport mode access
 access-session closed
 access-session port-control auto
 dot1x pae authenticaton
 service-policy type control subscriber simple_dot1x
!
```

```
interface Vlan22
 ip address 198.51.100.1 198.51.100.254
```

Configure device tracking

```
!
device-tracking policy tracking_test
 security-level glean
 no protocol ndp
 no protocol dhcp6
 tracking enable
!
interface GigabitEthernet0/1/7
 device-tracking attach-policy tracking_test
```

SHDSL Commands

- ```
  Router# config-transaction
  Router(config)# controller shdsl 0/1/0
  Router(config-controller)# termination cpe
  ```

- ```
  Router# config-transaction
  Router(config)# controller shdsl 0/1/0
  Router(config-controller)# termination <cpe/co>
  Router(config-controller)# mode atm
  ```

- ```
  Router# config-transaction
  Router(config)# controller shdsl 0/1/0
  Router(config-controller)# termination cpe
  Router(config-controller)# mode efm
  ```

- ```
  Router# config-transaction
  Router(config)# controller shdsl 0/1/0
  Router(config-controller)# termination cpe
  Router(config-controller)# mode atm
  Router(config-controller)# dsl-group 0 pairs 0
  Router(config-controller-dsl-group)#
  ```

- ```
  Router# config-transaction
  Router(config)# controller shdsl 0/1/0
  Router(config-controller)# termination cpe
  Router(config-controller)# mode atm
  Router(config-controller)# dsl-group auto
  Router(config-controller-dsl-group)#
  ```

- ```
  Router(config)# controller shdsl 0/1/0
  Router(config-controller)# termination cpe
  Router(config-controller)# mode atm
  Router(config-controller)# dsl-group 0 pairs 0-3 m-pair
  Router(config-controller-dsl-group)#
  ```

- ```
  Router(config)# controller shdsl 0/1/0
  Router(config-controller)# termination cpe
  Router(config-controller)# mode efm
  Router(config-controller)# dsl-group 0 pairs 0-3 efm-bond
  Router(config-controller-dsl-group)#
  ```

- ```
  Router(config)# controller shdsl 0/1/0
  Router(config-controller)# termination cpe
  Router(config-controller)# mode atm
  Router(config-controller)# dsl-group 0 pairs 0
  Router(config-controller)# dsl-group 1 pairs 2-3 m-pair
  ```

```
Router(config)# controller shdsl 0/1/0
Router(config-controller)# termination cpe
Router(config-controller)# mode efm
Router(config-controller)# dsl-group 0 pairs 0
Router(config-controller)# dsl-group 1 pairs 1-2 efm-bond
Router(config-controller)# dsl-group 3 pairs 3
```

- ```
  Router# configure terminal
  Enter configuration commands, one per line. End with CNTL/Z.
  Router(config)#controller shdsl 0/1/0
  Router(config-controller)#firmware phy?
  filename filename to read firmware

  Router(config-controller)# firmware phy filename ?

  flash: Download fw file name
  bootflash: Download fw file name

  Router(config-controller)#firmware phy filename
  bootflash:IDC_192.0.2.1_DFE_1.1-1.8.1__001.pkg
  ```

- ```
  shdsl annex { annex standard } [ coding < tcpam >]



  Router(config-controller-dsl-group)# shdsl annex ?

  A Annex A of G.991.2 standard
  A-F Annex A/F of G.991.2 standard
  B Annex B of G.991.2 standard
  B-G Annex B/G of G.991.2 standard
  F Annex F of G.991.2 standard
  G Annex G of G.991.2 standard

  Router(config-controller-dsl-group)# shdsl annex F coding ?

  128-TCPAM 128-TCPAM line coding
  16-TCPAM 16-TCPAM line coding
  32-TCPAM 32-TCPAM line coding
  4-TCPAM 4-TCPAM line coding
  64-TCPAM 64-TCPAM line coding
  8-TCPAM 8-TCPAM line coding


  Router(config-controller-dsl-group)# shdsl annex F coding 32-TCPAM
  ```

- ```
  Router (config-controller-dsl-group)# shdsl rate <rate>
  ```

- ```
  Router(config-controller-dsl-group)# handshake ?

  auto Initiate auto handshake
  ieee Initiate IEEE handshake
  itut Initiate ITUT handshake
  ```

- ```
  CPE(config-controller-dsl-group)# shdsl 4-wire mode enhanced
  ```

- ```
  CPE(config-controller-dsl-group)# ignore
  ```

- ```
  CPE(config-controller-dsl-group)# shutdown
  ```

SNMP Commands

- ```
  snmp-server packetsize <>
  ```

- snmp-server view supriya iso <>
- snmp-server user SNMP_V3_User SNMP_Group_Name v3 auth sha sha_pwd priv aes 128 aes_pwd access ipv6 <>
- snmp-server engineID local <123456ABCD>
- snmp mib community-map SNMP_V2c_Community_String engineid <12345ABCD6>
- snmp-server community <>
- snmp-server community MyROCommunity ro <>
- snmp-server community someword1 view someword2 ro <>
- snmp-server group someword v3 priv read someword access <>
- snmp-server group someword v3 priv read someword access ipv6 <>
- snmp-server file-transfer access-group <>
- snmp-server enable traps snmp authentication
- snmp-server enable traps snmp coldstart
- snmp-server enable traps snmp linkdown
- snmp-server enable traps snmp linkup
- snmp-server enable traps snmp warmstart

TCP Commands

- service tcp-keepalives-in
- service tcp-keepalives-out
- service tcp-small-servers
- service udp-small-servers
- ip finger

VDSL Commands

- config-transaction

  controller VDSL slot/subslot/port

  operating mode auto
- line-mode single-wire line line-number
- line-mode bonding
- Router# config-transaction
  Enter configuration commands, one per line. End with CNTL/Z.
  Router(config)#controller shdsl 0/1/0
  Router(config-controller)#firmware phy?
  filename filename to read firmware

  Router(config-controller)# firmware phy filename ?

- sra
- bitswap
- modem <keyword>
- description <string>
- diagnostics DELT
- training log filename flash:<filename>
- sync mode
- sync interval

Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.4.1a

Table 120: Feature History

Feature Name	Release Information	Description
Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Cisco IOS XE Catalyst SD-WAN Release 17.4.1a Cisco vManage Release 20.4.1	Starting Cisco IOS XE Catalyst SD-WAN Release 17.4.1a, you can use additional commands in CLI Add-on feature templates.

AAA and DOT1X Global Configuration

```
aaa group server radius radius-0
 server-private {ise_server} auth-port 1812 acct-port 1813 timeout 5 retransmit 3 key
cisco123

aaa authorization network default group radius-0
aaa authentication dot1x default group radius-0
aaa accounting dot1x default start-stop group radius-0

dot1x system-auth-control
radius-server dead-criteria time 10 tries 3
radius-server deadtime 15
```

AAA Tacacs and Radius

```
aaa group server radius rad123
 server-private 10.255.255.254
ip radius source-interface GigabitEthernet0/0/1
 radius-server key 0
$CRYPT_CLUSTER$a8YJvVLAFYXnoYOhLUMO5Q==$6tofKux6yYsQ42+nYL9FGf3wg4cKWLxB4O5zdWoFvmY=
aaa group server tacacs+ tac123
 server-private 10.255.255.254 key 0
$CRYPT_CLUSTER$a8YJvVLAFYXnoYOhLUMO5Q==$6tofKux6yYsQ42+nYL9FGf3wg4cKWLxB4O5zdWoFvmY=
ip tacacs source-interface GigabitEthernet0/0/1
aaa authentication login default group rad123 group tac123 local
username admin privilege 15 secret 5 $1$XQJ4$VxlKu0qZFDzNz8PjZqFSF1
```

CFM CLI List

```
ethernet cfm ieee
ethernet cfm global
ethernet cfm traceroute cache
ethernet cfm logging
ethernet cfm traceroute cache size entries
ethernet cfm traceroute cache hold-time minutes
snmp-server enable traps ethernet cfm cc
snmp-server enable traps ethernet cfm crosscheck
ethernet evc evc-id
ethernet cfm domain domain-name level level-id
 id dns dns-name
 mep ccm-hold-time hours
 mep ccm-fastage enable
 mep archive-hold-time minutes
 sender-id chassis
 service vpn-id vpn-id port
 service vlan-id vlan-id port
 service number MA-number port
 service short-ma-name port
 service short-ma-name evc evc-name vlan vlanid direction down
  continuity-check
  continuity-check [interval cc-interval]
  continuity-check loss-threshold threshold
  ais period 1 or 60
  ais level 0-7
  ais expiry-threshold 0-255
  ais suppress-alarms
  maximum meps 1-65535
  sender-id chassis
  offload sampling sample
Interface interface-name
 cfm mep domain domain-name mpid id service service-name
  alarm notification all*
  cos 0-7
 ethernet oam
 ethernet oam mode passive
 ethernet oam remote-loopback supported
 ethernet loopback permit external
```

CXP Branch DIA

```
class-map match-any ART_APPLICATIONS
 match protocol attribute application-group ms-cloud-group
!
performance monitor context sdwanarts profile sdwan-performance
 exporter destination local-sdwan source Null0
 traffic-monitor art-cor-saas class-and ART_APPLICATIONS ipv4
!
performance monitor sampling-rate 10
performance monitor apply sdwanarts color-all-dia|color
!
```

CXP Gateway

```
class-map match-any ART_APPLICATIONS
 match protocol attribute application-group ms-cloud-group
!
performance monitor context sdwanarts profile sdwan-performance
 exporter destination local-sdwan source Null0
 traffic-monitor art-cor-saas class-and ART_APPLICATIONS ipv4
!
performance monitor sampling-rate 10
```

```
interface GigabitEthernetx/x/x
 performance monitor context sdwanarts
!
```

DSL NIM Support

```
controller VDSL 0/1/0
line-mode single-wire line
no shutdown/shutdown
operating mode auto/adsl1/adsl2/adsl2+/auto adsl/auto adsl2/auto adsl2+/vdsl2
sra
bitswap
description VADSL_Ping_Test
training log filename bootflash:testlog.bin
firmware phy filename bootflash:nim_vab_phy_fw_A38q_B39x3.pkg
!
interface ATM0/1/0
description Atm_Main_intf
no shutdown
ip mtu 1500
mtu 1500
!
interface ATM0/1/0.303 point-to-point
description Atm_Sub_intf
no shutdown
ip address 192.0.2.254 255.255.255.0
ip mtu 1492
pvc 20/60
encapsulation aal5snap/aal5mux ppp dialer
protocol ppp dialer/dialer pool-member 1
!
!
interface Ethernet0/1/0
description Ethernet_Main_intf
no shutdown
mtu 1500
!
interface Ethernet0/1/0.303
description Ethernet_Sub_intf
no shutdown
encapsulation dot1Q 303
ip address 192.0.2.254 255.255.255.0
ip mtu 1492
pppoe enable
pppoe-client dial-pool-number 30
pppoe-client ppp-max-payload 1708
!
interface GigabitEthernet0/0/0
no shutdown
arp timeout 1200
ip address 192.0.2.254 255.255.255.0
no ip redirects
ip mtu 1500
mtu 1500
negotiation auto
!
interface Loopback1
description intf_loop_1
no shutdown
ip address 192.0.2.254 255.255.255.0
!
interface Loopback2
description intf_loop_2
no shutdown
```

```
ip address 192.0.2.254 255.255.255.0
!
interface Dialer30
no shutdown
encapsulation ppp
ip unnumbered Loopback1/Loopback2/GigabitEthernet0/0/0
dialer pool 30
ppp chap hostname cisco
ppp chap password 0 sisco
ppp pap sent-username cisco password sisco
ppp authentication chap pap callin
!
interface Tunnel0
no shutdown
ip unnumbered GigabitEthernet0/0/0
no ip redirects
ipv6 unnumbered GigabitEthernet0/0/0
no ipv6 redirects
tunnel source GigabitEthernet0/0/0
tunnel mode sdwan
!
interface Tunnel3
no shutdown
ip unnumbered Dialer30
tunnel source Dialer30
tunnel mode sdwan
!
sdwan
interface GigabitEthernet0/0/0
tunnel-interface
encapsulation ipsec weight 1
no border
color mpls
no last-resort-circuit
no low-bandwidth-link
no vbond-as-stun-server
vmanage-connection-preference 5
port-hop
carrier default
nat-refresh-interval 5
hello-interval 1000
hello-tolerance 12
allow-service all
no allow-service bgp
allow-service dhcp
allow-service dns
allow-service icmp
allow-service sshd
allow-service netconf
no allow-service ntp
no allow-service ospf
no allow-service stun
allow-service https
no allow-service snmp
no allow-service bfd
!
interface Dialer30
tunnel-interface
encapsulation ipsec
color biz-internet
allow-service all
no allow-service bgp
allow-service dhcp
allow-service dns
```

```
allow-service icmp
allow-service sshd
allow-service netconf
no allow-service ntp
no allow-service ospf
no allow-service stun
allow-service https
no allow-service snmp
no allow-service bfd
!
!
```

FNF Support for IPv6

```
app-visibility-ipv6
flow-visibility-ipv6
ip visibility cache entries
ipv6 visibility cache entries
```

GRE/IPSec LoadBalancing Using ECMP to Zscaler ZEN Node

```
interface Tunnel100512
 tunnel route-via GigabitEthernet1 mandatory
ip sdwan route vrf 1 0.0.0.0/0 service sig
sdwan service sig vrf global
 ha-pairs
  interface-pair Tunnel100511 active-interface-weight 100 Tunnel100512 backup-interface-weight
 200
```

IPSLA IPv4

```
ip sla 1
  icmp-echo 203.0.113.255
  vrf 100
ip sla schedule 1 life forever start-time now
track 1 ip sla 1 state
ip sla 2
  icmp-echo 203.0.113.255
  vrf 300
ip sla schedule 2 life forever start-time now
track 2 ip sla 2 state
ip access-list extended test300
 100 permit ip any 203.0.113.255 255.255.255.0
ip access-list extended test100
 100 permit ip any 192.0.2.254 255.255.255.0
!
class-map match-any test300
 match access-group name test300
class-map match-any test100
 match access-group name test100
!
policy-map type epbr test300
 class test300
  set ipv4 vrf 300 next-hop verify-availability 192.0.2.254 10 track 2
policy-map type epbr test100
 class test100
  set ipv4 vrf 100 next-hop verify-availability 192.0.2.254 10 track 1
!
interface GigabitEthernet0/0/1
 service-policy type epbr input test300
interface GigabitEthernet0/0/2
 service-policy type epbr input test100
!
```

IPv4 EPBR

```
ip access-list extended test300
 100 permit ip any 0.0.0.2 255.255.255.0
ip access-list extended test100
 100 permit ip any 0.0.0.2 255.255.255.0
!
class-map match-any test300
 match access-group name test300
class-map match-any test100
 match access-group name test100
!
policy-map type epbr test300
 class test300
  set ipv4 vrf 300 next-hop 203.0.113.255
policy-map type epbr test100
 class test100
  set ipv4 vrf 100 next-hop 203.0.113.255
!
interface GigabitEthernet0/0/1
 service-policy type epbr input test300
interface GigabitEthernet0/0/2
 service-policy type epbr input test100
```

IPv6 EPBR

```
ipv6 access-list test300_v6
  sequence 100 permit ipv6 any 2003::2/64
ipv6 access-list test100_v6
 sequence 100 permit ipv6 any 2001::2/64
!
class-map match-any test300_v6
 match access-group name test300_v6
class-map match-any test100_v6
 match access-group name test100_v6
!
policy-map type epbr test300_v6
 class test300_v6
  set ipv6 vrf 300 next-hop 2003::2
policy-map type epbr test100_v6
 class test100_v6
  set ipv6 vrf 100 next-hop 2001::2
!
interface GigabitEthernet0/0/1
 service-policy type epbr input test300_v6
interface GigabitEthernet0/0/2
 service-policy type epbr input test100_v6
```

Loopback Ports

```
interface Loopback100
 ip mtu 2000
```

Multi-SN (SC CLI List)

```
vrf definition 300
rd 1:300
address-family ipv4
route-target export 1:300
route-target import 1:300
exit-address-family
!
address-family ipv6
```

```
exit-address-family
interface TenGigabitEthernet0/1/2
no shutdown
arp timeout 1200
vrf forwarding 300
ip address 10.255.255.254 255.255.255.0
ip mtu 1496
ip nbar protocol-discovery
mtu 1500
exit
service-insertion appnav-controller-group appqoe ACG-APPQOE
appnav-controller 10.255.255.254 vrf 300
!
service-insertion service-node-group appqoe SNG-APPQOE
service-node 10.255.255.254
service-node 10.255.255.254
!
service-insertion service-context appqoe/1
appnav-controller-group ACG-APPQOE
service-node-group SNG-APPQOE
cluster-type service-controller
enable
vrf global
!
policy
app-visibility
app-visibility-ipv6
flow-visibility
flow-visibility-ipv6
no implicit-acl-logging
log-frequency 1000
!
```

Multi-SN (SN CLI List)

```
interface GigabitEthernet2
no shutdown
arp timeout 1200
ip address 10.255.255.254 255.255.255.0
no ip redirects
ip mtu 1500
mtu 1500
negotiation auto
interface VirtualPortGroup2
no shutdown
ip address 192.168.2.1 255.255.255.0
service-insertion appqoe
service-insertion service-node-group appqoe SNG-APPQOE
device-role service-node
service-node 192.168.2.2
```

Per-Class App Aware Routing

```
policy
sla-class sla1
loss 10
jitter 10
latency 10
app-probe-class apc1
!
sla-class sla2
loss 50
jitter 50
```

```
latency 50
app-probe-class apc2
!
app-route-policy _vpn_1_list_perclassaar_policy_vpn_1_list
vpn-list vpn_1_list
sequence 1
match
source-ip 10.0.0.0/8
!
action
sla-class sla1
!
!
sequence 11
match
source-ip 10.0.0.0/8
!
action
count counter2
sla-class sla1
!
!
default-action sla-class sla2
!
lists
site-list site_all_app_regr
site-id 100
site-id 400
site-id 500
site-id 600
!
app-probe-class apc1
forwarding-class class3
color lte dscp 10
color 3g dscp 11
color red dscp 12
color gold dscp 13
!
app-probe-class apc2
forwarding-class class5
color lte dscp 20
color 3g dscp 21
!
vpn-list vpn_1_list
vpn 1
!
!
!
apply-policy
site-list site_all_app_regr
app-route-policy _vpn_1_list_perclassaar_policy_vpn_1_list
bfd color lte
dscp 35
bfd color 3g
dscp 36
bfd default-dscp 28
!
!
```

PMTU Configuration

```
bfd color lte
hello-interval 1000
```

```
pmtu-discovery
multiplier 1
```

POE

```
interface {intf-name}
power inline auto max <4000-60000>
power inline auto
power inline never
```

Policy Based SIG

```
policy
data-policy sig_ha_zscaler_data_policy_vedg
  vpn-list vpn_1
   sequence 90
    match
     destination-ip 10.255.255.254/32
    action accept
     count seqcnt_90
     sig
   sequence 100
    match
     destination-ip 10.255.255.254/32
    action accept
     count seqcnt_100
     sig
   sequence 110
    match
     destination-ip 10.255.255.254/32
    action accept
     count seqcnt-110
     sig
   default-action accept
 lists
  vpn-list vpn_1
   vpn 1
  site-list vedge_1
   site-id 500
   site-id 600
apply-policy
 site-list vedge_1
  data-policy sig_ha_zscaler_data_policy_vedg from-service
```

Routed Ports

```
interface GigabitEthernet0/0/1
ip mtu 9000
mtu 9216
```

SLA IPv6

```
ip sla 3
  icmp-echo 2001::2
  vrf 100
ip sla schedule 3 life forever start-time now
track 3 ip sla 3 state
ip sla 4
  icmp-echo 2003::2
  vrf 300
ip sla schedule 4 life forever start-time now
track 4 ip sla 4 state
ipv6 access-list test300_v6
```

```
  sequence 100 permit ipv6 any 2003::2/64
ipv6 access-list test100_v6
 sequence 100 permit ipv6 any 2001::2/64
!
class-map match-any test300_v6
 match access-group name test300_v6
class-map match-any test100_v6
 match access-group name test100_v6
!
policy-map type epbr test300_v6
 class test300_v6
  set ipv6 vrf 300 next-hop verify-availability 2003::2 10 track 4
policy-map type epbr test100_v6
 class test100_v6
  set ipv6 vrf 100 next-hop verify-availability 2001::2 10 track 3
!
!
interface GigabitEthernet0/0/1
 service-policy type epbr input test300_v6
interface GigabitEthernet0/0/2
 service-policy type epbr input test100_v6
!
```

SNMP

- snmp-server community 0 $CRYPT_CLUSTER$IXnkuKPGacBNK+bXDmIq4Q==$msxENYwt8IX5ylClfcb+rA== view 4431_view ro
  snmp-server host 10.255.255.254 0 $CRYPT_CLUSTER$IXnkuKPGacBNK+bXDmIq4Q==$msxENYwt8IX5ylClfcb+rA== udp-port 100 version 2csnmp-server view 4431_view iso included

- snmp-server host 10.255.255.254 vrf Mgmt-intf 0 $CRYPT_CLUSTER$IXnkuKPGacBNK+bXDmIq4Q==$msxENYwt8IX5ylClfcb+rA==snmp-server host 10.255.255.254 vrf Mgmt-intf 0 $CRYPT_CLUSTER$IXnkuKPGacBNK+bXDmIq4Q==$msxENYwt8IX5ylClfcb+rA== udp-port 15

- snmp-server host 10.1.1.1 vrf vrf-name informs version 2c priv 0 $CRYPT_CLUSTER$IXnkuKPGacBNK+bXDmIq4Q==$msxENYwt8IX5ylClfcb+rA== udp-port 15

- snmp mib community-map 0 $CRYPT_CLUSTER$IXnkuKPGacBNK+bXDmIq4Q==$msxENYwt8IX5ylClfcb+rA==

- snmp-server community 0 $CRYPT_CLUSTER$IXnkuKPGacBNK+bXDmIq4Q==$msxENYwt8IX5ylClfcb+rA==> ro acl-name

Spanning Tree

```
spanning-tree mode rapid-pvst
interface {intf-name}
spanning-tree portfast
```

SVI Ports

```
interface Vlan25
ip mtu 1600
```

Switchport Interface Configuration

- interface {intf-name}
  switchport mode access
  switchport access vlan {vlan_id}
  dot1x pae authenticator
  authentication order dot1x mab

```
authentication host-mode single-host
authentication port-control auto
authentication timer reauthenticate <timer_num/server>
authentication timer inactivity <timer_num/server>
authentication event server dead action authorize vlan {critical_vlan}
authentication event fail action authorize vlan {restrict_vlan}
authentication event no-response action authorize vlan {guest_vlan}
no shutdown
```

- ```
  interface {intf-name}
  speed {value}
  duplex {value}
  mtu {value}
  switchport mode trunk
  switchport trunk allowed vlan {vlans}
  switchport trunk native vlan {vlans_id}
  no shutdown
  ```

- ```
  mac address-table static {mac1} vlan {intf_vlan} interface {intf_name}
  ```

Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.5.1a

Table 121: Feature History

Feature Name	Release Information	Description
Qualified Commands for Cisco IOS XE Release 17.5.1	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Additional commands are qualified for use in Cisco vManage CLI templates.

Application-Aware Routing

```
fallback-best-tunnel
criteria jitter
```

Application Performance Monitoring

```
performance monitor context 175_SDWAN profile sdwan-performance
exporter destination 10.0.1.128 source GigabitEthernet9 port 2055
traffic-monitor application-response-time
traffic-monitor media
!
performance monitor apply 175_SDWAN sdwan-tunnel
```

Multicast PIM BSR Dynamic RP

```
ip pim vrf 1 bsr-candidate GigabitEthernet5
ip pim vrf 1 rp-address 172.16.255.116
ip pim vrf 1 rp-candidate GigabitEthernet5 interval 10 priority 5

ip pim sparse-mode

spt-only
```

Data Policy Next-hop

```
next-hop-loose
```

DCA

```
platform resource service-plane-heavy
platform resource data-plane-heavy
```

DIA - DDOS Visibility

```
policy
implicit-acl-logging
log-frequency  <int value>
```

DRE

Service Node Configuration

```
interface VirtualPortGroup2
no shutdown
ip address 192.168.2.1 255.255.255.0
service-insertion appqoe
exit
interface VirtualPortGroup3
no shutdown
ip address 192.168.3.1 255.255.255.252
exit

app-hosting appid dreopt
app-vnic gateway0 virtualportgroup 3 guest-interface 1
guest-ipaddress 192.168.3.2 netmask 255.255.255.252
!
start
!

dual-side optimization enable
```

Integrated Service Node Configuration

```
interface VirtualPortGroup2
no shutdown
ip address 192.168.2.1 255.255.255.0
service-insertion appqoe
exit
interface VirtualPortGroup3
no shutdown
ip address 192.168.3.1 255.255.255.252

service-insertion appnav-controller-group appqoe ACG-APPQOE
appnav-controller 192.168.2.1
!
service-insertion service-node-group appqoe SNG-APPQOE
service-node 192.168.2.2
!
service-insertion service-context appqoe/1
appnav-controller-group ACG-APPQOE
service-node-group SNG-APPQOE
cluster-type integrated-service-node
enable
vrf global
!
iox
app-hosting appid dreopt
```

```
app-vnic gateway0 virtualportgroup 3 guest-interface 1
guest-ipaddress 192.168.3.2 netmask 255.255.255.252
!
start
!
dreopt enable
!
dual-side optimization enable
!
```

Office 365: Dynamic NBAR Mapping

```
service-area exchange
```

Geo Filter

```
object-group geo DST_GEO_LIST1
 country FLK
 country UZB
 country YEM
!
object-group geo SELF_ZONE_RULES-seq-Rule_5-geo-dstn-og_
 country MYT
 country TCD
 continent OC
!
object-group geo master-seq-Rule_11-geo-dstn-og_
 group-object DST_GEO_LIST1
!

object-group geo master-seq-Rule_11-geo-src-og_
 group-object GEO_SRC_LIS1
 group-object GEO_SRC_LIST2
!
object-group geo ruleset-RS4-R1-geo-dstn-og_
 continent NA
!
object-group geo ruleset-RS5-R1-geo-dstn-og_
 country FIN
 country FRA
!
ip access-list extended LAN_to_WAN_and_DIA-seq-Rule_11-acl_
 17 permit object-group LAN_to_WAN_and_DIA-seq-Rule_11-service-og_ geo-group
master-seq-Rule_11-geo-src-og_ object-group master-seq-Rule_11-network-dstn-og_
 18 permit object-group LAN_to_WAN_and_DIA-seq-Rule_11-service-og_ geo-group
master-seq-Rule_11-geo-src-og_ fqdn-group master-seq-Rule_11-fqdn-dstn-og_
 19 permit object-group LAN_to_WAN_and_DIA-seq-Rule_11-service-og_ geo-group
master-seq-Rule_11-geo-src-og_ geo-group master-seq-Rule_11-geo-dstn-og_
!
ip access-list extended SELF_ZONE_RULES-seq-Rule_5-acl_
 15 permit object-group SELF_ZONE_RULES-seq-Rule_5-service-og_ any geo-group
SELF_ZONE_RULES-seq-Rule_5-geo-dstn-og_
!
ip access-list extended ruleset-RS4-acl_
 175 permit object-group ruleset-RS4-R1-service-og_ geo-group ruleset-RS4-R1-geo-src-og_
object-group master-ruleset-RS4-R1-network-dstn-og_
 200 permit object-group ruleset-RS4-R1-service-og_ geo-group ruleset-RS4-R1-geo-src-og_
fqdn-group master-ruleset-RS4-R1-fqdn-dstn-og_
 225 permit object-group ruleset-RS4-R1-service-og_ geo-group ruleset-RS4-R1-geo-src-og_
geo-group ruleset-RS4-R1-geo-dstn-og_
!
ip access-list extended ruleset-RS5-acl_
 125 permit object-group ruleset-RS5-R1-service-og_ any geo-group ruleset-RS5-R1-geo-dstn-og_
```

```
!
geo database
```

GRE Tunnel from the Service Side

```
interface Tunnel100512
no shutdown
vrf forwarding 1
ip address 192.168.0.1 255.255.255.248
no ip clear-dont-fragment
ip tcp adjust-mss 1387
ip mtu              1500
tunnel source 10.0.3.55
tunnel destination 10.0.3.149
exit
```



Note This can also be used with an Amazon Web Services (AWS) transit gateway (TGW) running a GRE tunnel.

NetAdmin

Authorization

```
aaa authorization console
aaa authorization config-commands
aaa authorization exec default group tacacs-0 local
aaa authorization commands 15 default group tacacs-0 if-authenticated
```

Accounting

```
aaa accounting exec default start-stop group tacacs-0
aaa accounting commands 15 default start-stop group tacacs-0
aaa accounting commands 1 default start-stop group tacacs-0
aaa accounting network default start-stop group tacacs-0
aaa accounting system default start-stop group tacacs-0
```

PPPoE

- `bandwidth 500`
- `bandwidth qos-reference 100000`
- ```
  ip access-group 1 out
  ipv6 enable
  keepalive 60
  ```
- `ppp ipcp mask request`
- `ppp ipcp dns request`

Security

```
snmp
no shutdown
view v2
oid 1.3.6.1
!
view v3
oid 1.3.6.1
!
```
```

```
community $CRYPT_CLUSTER$i7nR7D99DSlEy4fF/WLdKA==$Vi0BKsnRfjxxiniO4bGutg==
view v2
authorization read-only
!
community $CRYPT_CLUSTER$kISnggeJ63senHxHbOCp0g==$PQAGFWVSrWCPpLJ5Au1mYw==
view v3
authorization read-only
!
ipv6 shutdown
```

Service Side Static NAT

Static NAT Inside Mapped to Inside Pool

```
ip nat pool natpool1 10.11.11.1 10.11.11.30 prefix-length 27
ip nat inside source list global-list pool natpool1 vrf 1 match-in-vrf overload
!
ip nat inside source static 192.168.11.10 11.11.11.10 vrf 1 match-in-vrf pool natpool1
```

Static NAT Outside Mapped to Outside Pool

```
ip nat pool natpool1 10.21.21.1 10.21.21.30 prefix-length 27
ip nat outside source list global-list pool natpool1 vrf 1 overload match-in-vrf
!
ip nat outside source static 192.168.21.10 10.21.21.10 vrf 1 match-in-vrf pool natpool1
```

Port-forwarding Mapped to Inside Pool

```
ip nat pool natpool1 10.11.11.1 10.11.11.30 prefix-length 27
ip nat inside source list global-list pool natpool1 vrf 1 match-in-vrf overload
!
ip nat inside source static tcp 192.168.11.10 80 10.11.11.10 8080 vrf 1 match-in-vrf pool
natpool1
```

SLE

Direct Connect Mode

```
license smart transport smart
license smart url smart https://smartreceiver-stage.cisco.com/licservice/license
ip name-server  172.16.168.183
ip http client source-interface GigabitEthernet0/0/2
```

Indirect Connect Mode

```
license smart transport cslu
license smart url cslu http:10.195.85.83:8182/cslu/v1/pi
ip name-server 172.20.168.183
ip http client source-interface GigabitEthernet0/0/2
```

Indirect Connect Mode

```
license smart transport off
```

Spanning Tree

```
spanning-tree guard root
spanning-tree bpdu guard enable
```

TCP MSS

```
ip tcp adjust-mss 1300
```

TrustSec

```
ip access-list role-based CTS_ACCESS_LIST
 10 permit ip
 20 permit tcp
 30 deny icmp
!
aaa group server radius radius-1
 server-private 77.251.1.1 timeout 5 retransmit 3 pac key 6 cd[UCLCiMIM^HTXbigAKUf[VJKJPSOQfD

 ip radius source-interface GigabitEthernet0/0/2
 ip vrf forwarding 1
!
aaa server radius dynamic-author
 client 77.251.1.1 vrf 1 server-key 6 gWTLbecJKOQcFcIbJNR[]WKP_g^TRacRF
!
key chain key1 tcp
 key 1000
  cryptographic-algorithm hmac-sha-256
  key-string 6 _RPB[dVI]SO^BAOVNMKATgOZKMXFGXFTa
  accept-lifetime local 18:00:00 Jan 12 2021 06:00:00 Jan 12 2022
  send-lifetime local 18:00:00 Jan 12 2021 01:00:00 Jan 12 2022
  send-id 215
  recv-id 215
  exit
!
cts authorization list cts-mlist
cts role-based permissions from 300 to 500 CTS_ACCESS_LIST
cts role-based enforcement
cts role-based sgt-map vrf 1 77.29.1.2 sgt 5
cts role-based sgt-map vrf 1 77.29.1.4 sgt 10
cts sxp node-id ipv4 77.29.1.1
cts sxp default password 6 LZcdEUScdLSVZceMAJ_R[cJgb^NbWNLLC
cts sxp default source-ip 77.29.1.1
cts sxp default key-chain key1
cts sxp connection peer 77.201.1.2 source 77.29.1.1 password key-chain mode local both vrf
 1
cts sxp enable
cts credentials id cEDGE4 password 6 RX^ASQVgfFV^EOAeQWVZ]VFQ_hcLDdgJJ
```

Interface Level Enforcement

```
cts role-based enforcement
```

Voice

```
rel1xx disable
header-passing
```

Commands Under Interface Serial

```
[no] cdp enable
snmp ifindex <clear | persist>
```

ISDN Commands Under Interface Serial

```
isdn map address <digit-string> plan [data | isdn | national | privacy | reserved/10 |
reserved/11 |
reserved/12 | reserved/13 | reserved/14 | reserved/2 | reserved/5 | reserved/6 | reserved/7
 | telex |
unknown] type [abbreviated | international | national | reserved/5 | subscriber | unknown]
```

```
isdn outgoing ie <called-number | called-subaddr | caller-number | caller-subaddr |
connected-number |
 connected-subaddr | display |  extended-facility | facility | high-layer-compat |
low-layer-compat |
```

Commands Under Trunk Group Hunt-Scheme

```
hunt-scheme <least-used | round-robin | sequential> [both | even | odd] [up | down]
```

SCCP Commands

```
bind interface <interface-name-slot/bay/port>
keepalive retries <1-32> default 3
keepalive timeout <0-180> default 10

sccp ip precedence <1-7> default is 5
```

Weighted Load Balancing for SaaS Traffic

```
probe-path load-balance-dia latency-variance 50
probe-path load-balance-dia loss-variance 30
probe-path load-balance-dia source-ip-hash false
```

Zscaler Location Based API

```
zscaler-location-settings
datacenters primary-data-center vie1-vpn.zscalerthree.net
auth-required false
ssl-scan-enabled false
xff-forward-enabled false
surrogate ip false
surrogate idle-time 0
surrogate display-time-unit MINUTE
surrogate ip-enforced-for-known-browsers false
surrogate refresh-time 0
surrogate refresh-time-unit MINUTE
ofw-enabled false
ips-control false
aup disabled
aup block-internet-until-accepted false
aup force-ssl-inspection false
aup timeout 0
caution-enabled false
!
tunnel-options tunnel-set secure-internet-gateway-zscaler tunnel-dc-preference primary-dc
source-interface GigabitEthernet1
exit
tunnel-options tunnel-set secure-internet-gateway-zscaler tunnel-dc-preference secondary-dc
 source-interface GigabitEthernet2
exit
zscaler organization cisco-dev.com
zscaler partner-base-uri admin.zscalerthree.net/api/v1
zscaler partner-key SAGv4U2lwh9R
zscaler username sig-dev@cisco-dev.com
zscaler password $8$O0i/6etiDQSqcm+B4yetJDPaYBx1x0wQujnz3pqQG7s=
```

Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.6.1a

Table 122: Feature History

Feature Name	Release Information	Description
Qualified Configurations for Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Additional commands are qualified for use in Cisco vManage CLI templates.

IP SLA

```
ip sla responder

ip sla 6001
 udp-jitter 172.31.11.85 44444 source-ip 172.31.17.220 num-packets 100
  request-data-size 64
  tag 6001:UDP64 HNZ-H7Z
  frequency 300

ip sla schedule 6001 life forever start-time now
ip sla 7001
 icmp-echo 172.31.17.222 source-ip 172.31.17.216
  request-data-size 64
  tag 7001:AVAILABILITY DSO-D7S
  frequency 30

ip sla schedule 7001 life forever start-time now
ip sla reaction-configuration 6001 react rtt threshold-value 40 40 threshold-type immediate
 action-type trapAndTrigger
ip sla reaction-configuration 6001 react timeout threshold-type immediate action-type
trapAndTrigger
ip sla reaction-configuration 6001 react packetLossDS threshold-value 1 1 threshold-type
immediate action-type trapAndTrigger
ip sla reaction-configuration 6001 react packetLossSD threshold-value 1 1 threshold-type
immediate action-type trapAndTrigger
ip sla reaction-configuration 7001 react timeout threshold-type immediate action-type
trapAndTrigger
```

AppQoE for RA user

SD-WAN Datacenter

```
hostname SDWAN-DC-B40
!
interface Loopback1
description apple.com DC-LAN
vrf forwarding 10
ip address 196.168.1.1 255.255.255.0
end
!
interface Loopback2
description google.com DC-LAN
vrf forwarding 20
ip address 197.168.1.1 255.255.255.0
end
```

```
!
interface GigabitEthernet4
description shared-service VPN (RADIUS server)
vrf forwarding 1
ip address 77.27.11.1 255.255.255.0
end
!
interface GigabitEthernet2 -> Internet TLOC
 tunnel-interface
 encapsulation ipsec
 color biz-internet restrict
!
interface GigabitEthernet5 -> MPLS TLOC
 tunnel-interface
 encapsulation ipsec
 color mpls restrict
```

Interface Configuration

```
interface GigabitEthernet2
description INTERNET-LINK(TLOC)
ip address 77.27.5.2 255.255.255.0
ip nat outside
negotiation auto
end
!
interface GigabitEthernet2 -> Internet TLOC
 tunnel-interface
 encapsulation ipsec
 color biz-internet restrict
!
interface GigabitEthernet7 -> MPLS TLOC
 tunnel-interface
 encapsulation ipsec
 color mpls restrict
!
interface GigabitEthernet4
description shared-service VPN
vrf forwarding 1
ip address 77.27.13.1 255.255.255.0
end
```

DIA configuration

```
ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet2 overload

ip nat route vrf 10 0.0.0.0 0.0.0.0 global
```

IKEv2/IPsec FlexVPN RA server configuration with Preshared-key

```
crypto ikev2 profile prof

description RA-SERVER common profile
match identity remote email domain apple.com
match identity remote email domain google.com
authentication remote pre-share key cisco
authentication local pre-share key cisco
aaa authorization user psk list AUTHORIZE name-mangler server
virtual-template 1
!
crypto ipsec profile prof
set ikev2-profile prof
!
interface Virtual-Template1 type tunnel
no ip address
tunnel mode ipsec ipv4
```

```
tunnel protection ipsec profile prof
!
```

IKEv2/IPsec FlexVPN RA server configuration with PKI

```
For any PKI configuration to work properly, the "clock" of the device should be set.

All the devices in the topology should be sync using NTP and the "show ntp status" should
be synchronized.

cry key generate rsa modulus 2048 label test-key

crypto pki trustpoint tp
enrollment url http://10.0.149.205:80/certsrv/mscep/mscep.dll
usage ike
fingerprint 32AE15680731AD3E91A612A72A35419D
subject-name CN=R1 C=pki
revocation-check none
rsakeypair tp 2048
auto-enroll 80
end

crypto pki trustpoint tp
enrollment url http://10.0.149.205:80
end
```

Routes to push to RA clients

```
ip access-list standard 98 (For google.com)
10 permit 197.168.0.0 0.0.255.255
!
ip access-list standard 99 (For apple.com)
20 permit any
!
```

IP pools to assign IP to RA clients

```
ip local pool apple 10.0.0.4 10.0.0.10 (For apple.com)
ip local pool google 20.0.0.4 20.0.0.10 (For google.com)
!
```

AAA configuration

```
aaa new-model
!
aaa group server radius RADIUS_PSK
server-private 77.27.11.2 key cisco
ip vrf forwarding 1
ip radius source-interface GigabitEthernet4
!
aaa authorization network AUTHORIZE group RADIUS_PSK
!
```

PKI Server config

For any PKI configuration to work properly, the "clock" of the device should be set. All the devices in the topology should be sync using NTP and the "show ntp status" should be synchronized. PKI server should **`ip http server`** config as a prerequisite.

RootCA:

```
crypto pki server ROOTCA
database level complete
database archive pkcs12 password 0 cisco123
grant auto
hash sha256
```

```
lifetime certificate 365
auto-rollover 0 0 20
no shutdown

hostname SOHO-RA-CLIENT
```

Configuration for apple.com

```
interface Loopback1

description APPLE.COM client-LAN
vrf forwarding 10
ip address 199.168.1.1 255.255.255.0
!
interface GigabitEthernet3
description INTERNET LINK FOR APPLE.COM
ip address 192.167.1.33 255.255.255.0
end
!
ip access-list standard 99
10 permit 199.168.0.0 0.0.255.255
!
crypto ikev2 authorization policy apple
route set interface
route set access-list 99
!
crypto ikev2 authorization policy google
route set interface
route set access-list 98
!
crypto ikev2 profile apple
description RA-CLIENT profile for apple.com
match identity remote any
identity local email abc@apple.com
authentication remote pre-share key cisco
authentication local pre-share key cisco
aaa authorization group psk list mylist apple
!
crypto ipsec profile apple
set ikev2-profile apple
!
interface Tunnel10
description SVTI-TUNNEL for apple.com
vrf forwarding 10
ip address negotiated
tunnel source GigabitEthernet3
tunnel mode ipsec ipv4
tunnel destination 77.27.5.2
tunnel protection ipsec profile apple
end
!
```

Configuration for google.com

```
interface Loopback2

description GOOGLE.COM client-LAN
vrf forwarding 20
ip address 199.170.1.1 255.255.255.0
end
!
interface GigabitEthernet4
description INTERNET LINK FOR GOOGLE.COM
ip address 194.167.1.33 255.255.255.0
negotiation auto
no mop enabled
```

```
no mop sysid
end
!
ip access-list standard 98
10 permit 199.170.0.0 0.0.255.255
!
crypto ikev2 profile google
description RA-CLIENT profile for google.com
match identity remote any
identity local email xyz@google.com
authentication remote pre-share key cisco
authentication local pre-share key cisco
aaa authorization group psk list mylist google
!
crypto ipsec profile google
set ikev2-profile google
!
interface Tunnel20
description SVTI-TUNNEL for google.com
vrf forwarding 20
ip address negotiated
tunnel source GigabitEthernet4
tunnel mode ipsec ipv4
tunnel destination 77.27.5.2
tunnel protection ipsec profile google
end
!
```

Carrier Supporting Carrier

```
interface GigabitEthernet2

no shutdown
mpls bgp forwarding
ip address 10.1.17.15 255.255.255.0

interface GigabitEthernet3
no shutdown
mpls bgp forwarding
ip address 10.1.19.15 255.255.255.0

router bgp 10
bgp router-id 10.1.1.15
neighbor 10.1.17.14 remote-as 100
neighbor 10.1.19.16 remote-as 100

address-family ipv4 unicast
maximum-paths 4
neighbor 10.1.17.14 activate

neighbor 10.1.17.14 as-override
neighbor 10.1.17.14 allowas-in

neighbor 10.1.17.14 advertisement-interval 30
neighbor 10.1.17.14 send-label explicit-null
neighbor 10.1.19.16 activate
neighbor 10.1.19.16 advertisement-interval 30
neighbor 10.1.19.16 send-community both
neighbor 10.1.19.16 send-label explicit-null
redistribute connected
redistribute static
exit-address-family
!
```

Cisco SD-WAN Etherchannel

```
interface Port-channel2
 ip address 10.0.0.1 255.255.255.0
 no negotiation auto
!

interface GigabitEthernet2/1/0
 no ip address
 negotiation auto
 cdp enable
 channel-group 2
!
interface GigabitEthernet2/1/1
 no ip address
 negotiation auto
 cdp enable
 channel-group 2
!
```

Cloud onRamp Over SIG Tunnels

```
probe-path branch sig-tunnel-list Tunnel100015 Tunnel100016
probe-path branch all-auto-sig-tunnels
```

Collect-tos/DSCP

```
Policy
 cflowd-template cflowd_server
  flow-active-timeout    60
  flow-inactive-timeout  30
  flow-sampling-interval 10
  protocol               ipv4
  collector vpn 0 address 10.0.100.1 port 4739 transport transport_udp
 customized-ipv4-record-fields
   collect-tos
   collect-dscp-outputpath
```

Cloud onRamp-SaaS gateway interface

```
probe
vanalytics-url https://us01.cloudservice.cisco.com
saas office365_apps
saas amazon_aws_apps
saas box_net_apps
saas dropbox_apps
saas intuit_apps
saas concur_apps
saas google_apps
!
```

```
probe-path gateway color-list <color>
```

or

```
probe-path gateway color-list <color>
```

DRE Profiles

```
interface VirtualPortGroup3
 no shutdown
 ip address 192.168.3.1 255.255.255.252
exit
```

```
platform resource service-plane-heavy
iox
app-hosting appid dreopt
 app-resource package-profile medium
 app-vnic gateway0 virtualportgroup 3 guest-interface 1
  guest-ipaddress 192.168.3.2 netmask 255.255.255.252
 start
```

The following CLI command can be configured on a vSmart.

```
policy
 data-policy _v1_dataPolicy
  vpn-list v1
    sequence 1
     match
      …
     !

     action accept
      dre-optimization
     !
    !

  default-action drop
 !
```

Geofencing with SD-WAN Edges

```
system
 gps-location latitude 37.416399
 gps-location longitude -121.918717
 gps-location geo-fencing-enable
 gps-location geo-fencing-config
  geo-fencing-range 200
  sms
   sms-enable
   mobile-number +14080000000
   !
  !
 !
!
```

Implicit ACL on Loopback Interface

```
sdwan
interface Loopback100
  tunnel-interface
   [bind interface-name]
   encapsulation ipsec
   color mpls
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
   allow-service https
  exit
```

Per VPN QoS

```
class-map match-all Queue0
match qos-group 0
class-map match-all Queue2
match qos-group 2
class-map match-all Queue3
match qos-group 3
class-map match-all Queue5
match qos-group 5
class-map match-all Queue7
match qos-group 7
!

class-map match-any Tenant-1
match packet-tag 1 11 65535
match packet-tag 1 12 65535
!
class-map match-any VPN_100
match packet-tag 1 100 65535
!

policy-map qos_1_500000 // generate specific qos_1 policy for 500000kbps
class Queue0
  priority level 1
policer rate 100000000 // priority queue policer rate 100Mbps = 500Mbps * 20%
class Queue3
  bandwidth remaining ratio 30
class Queue7
  bandwidth remaining ratio 35
class class-default
  bandwidth remaining ratio 15
!

policy-map qos_1_300000 // generate specific qos_1 policy for 300000kbps
class Queue0
  priority level 1
policer rate 60000000 // priority queue policer rate 60Mbps = 300Mbps * 20%
class Queue3
  bandwidth remaining ratio 30
class Queue7
  bandwidth remaining ratio 35
class class-default
  bandwidth remaining ratio 15
!

policy-map qos_2_200000 // generate specific qos_2 policy for 200000kbps
class Queue0
  priority level 1
policer rate 70000000 // priority queue policer rate 70Mbps = 200Mbps * 35%
class Queue5
  bandwidth remaining ratio 45
class class-default
  bandwidth remaining ratio 20
!

policy-map VPN_Policy
class Tenant-1
  bandwidth remaining ratio 50 // configured bandwidth 500000kbps
   service-policy qos_1_500000
class VPN_100
  bandwidth remaining ratio 20 // configured bandwidth 200000kbps
shape average 300000000    // configured maximum bandwidth 300000kbps
   service-policy qos_2_200000
```

```
class class-default
  bandwidth remaining ratio 30 // rest of 300000kbps (1000000kbps – 500000kbps – 200000kbps)

   service-policy qos_1_300000
!

policy-map Phy_WAN_Policy
class class-default
  shape average 1000000000
   service-policy VPN_Policy
!

interface GigabitEthernet2
service-policy output Phy_WAN_Policy
!

sdwan
 vpn packet-tag 1



ipsec
rekey 86400
replay-window 512
extended-ar-window 256
authentication-type ah-sha1-hmac sha1-hmac
!
!
```

QoS Commands

```
policy
 cloud-qos
 cloud-qos-service-side
 class-map
  class Queue0 queue 0
  class Queue3 queue 3
  class Queue4 queue 4
  class queue4 queue 4
 !

 qos-scheduler ut-qos-222_0
  class Queue0
  bandwidth-percent 5
  buffer-percent 10
  scheduling llq
 !

 qos-scheduler ut-qos-222_3
  class Queue3
  bandwidth-percent 30
  buffer-percent 30
 !

 qos-scheduler ut-qos-222_4
  class Queue4
  bandwidth-percent 1
  buffer-percent 50
  drops red-drop
 !
 qos-map ut-qos-222
  qos-scheduler ut-qos-222_4
```

Route Leaking

```
track 1 ip route 12.1.1.0 255.255.255.0 reachability
 ip vrf red
```

vrrp-v3 configuration

```
interface GigabitEthernet7
 vrf forwarding 100
 ip address 13.1.1.1 255.255.255.0
 negotiation auto
 vrrp 2 address-family ipv4
  vrrpv2
  priority 220
  track 1 decrement 25
  preempt delay minimum 30
  address 13.1.1.100 primary
exit
```

vrf configuration

```
vrf definition 100
 !
 address-family ipv4
 exit-address-family
sdwan
  omp
    no shutdown
    graceful-restart
    no as-dot-notation
    timers
      holdtime               15
      graceful-restart-timer 120
exit
    address-family ipv4
       distance 100
       advertise bgp
    !
    address-family ipv6
      distance 100
      advertise bgp
    !
    address-family ipv4 vrf 1
       distance 200
       advertise bgp
    !
    address-family ipv6 vrf 1
      distance 200
      advertise bgp
    !
  !
```

SD-WAN Multitenancy

```
clear sdwan reverse-proxy context
clear sdwan certificate reverse-proxy
show sdwan certificate reverse-proxy
```

SNMP Commands

```
snmp ifmib ifindex persist
snmp-server community private view v3 ro 5
snmp-server community public view v2 ro
snmp-server contact MY_CONTACT_NAME
snmp-server context MY_CONTEXT
```

```
snmp-server enable traps alarms informational
snmp-server enable traps bgp state-changes limited
snmp-server enable traps config
snmp-server enable traps entity
snmp-server enable traps entity-state
snmp-server enable traps snmp authentication coldstart linkdown linkup warmstart
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps sdwan
snmp-server enable traps bgp state-changes limited
snmp-server group groupAuthNoPriv v3 auth read v3
snmp-server group groupAuthPriv v3 priv read v3
snmp-server group groupNoAuthNoPriv v3 noauth read v3
snmp-server host 172.27.54.199 vrf 172 version 2c public udp-port 162
snmp-server host 172.27.214.64 vrf 172 version 2c public udp-port 16664
snmp-server location sjc-20
snmp-server packetsize 1300
no snmp-server sparse-tables
no snmp-server trap authentication unknown-context
snmp-server trap-source Loopback0
snmp-server view v2 1.3.6.1 included
snmp-server view v3 1.3.6.1 included
snmp-server view v3 internet included
```

UCSE as AppQoE Service Node

```
platform resource app-heavy

service-insertion service-context appqoe/1
  cluster-type hybrid
  appnav-controller-group ACG-APPQOE
  service-node-group SNG-APPQOE1
  service-node-group SNG-APPQOE2
  vrf global
  enable

 !
```

Unified Security Policy

Policy CLI

```
parameter-map type inspect-global
log dropped-packets
multi-tenancy
vpn zone security
alert on
utd-policy AIP_1

parameter-map type inspect AIP_1-pmap_
utd-policy AIP_1

policy-map type inspect FW_UNIFIED_POLICY_1
class type inspect FW_UNIFIED_POLICY_1-seq-1-cm_
inspect AIP_1-pmap_
class class-default
drop

zone security ZONE_1_2
vpn 1
vpn 2
```

```
zone-pair security ZP_ZONE_1_2_ZONE_1_2_F_671459382 source ZONE_1_2 destination ZONE_1_2
service-policy type inspect FW_UNIFIED_POLICY_1
```

UTD CLI

```
utd engine standard unified-policy
web-filter block page profile block-URLF_UNIFIED_1
text Access to the requested page has been denied.Blocked by admin
web-filter url profile URLF_UNIFIED_1
alert all
categories block
sports
gambling
block page-profile block-URLF_UNIFIED_1
log level error
reputation
block-threshold low-risk
threat-inspection profile IPS_UNIFIED_1
threat detection
policy security
logging level info
utd global
file-analysis
apikey 0 <apikey>
cloud-server isr.api.threatgrid.eu
file-reputation
cloud-server cloud-isr-asn.amp.cisco.com
est-server cloud-isr-est.amp.cisco.com
file-analysis profile AMP_UNIFIED_1-fa-profile
alert level info
file-types
pdf
ms-exe
file-reputation profile AMP_UNIFIED_1-fr-profile
alert level info
file-inspection profile AMP_UNIFIED_1-fi-profile
reputation profile AMP_UNIFIED_1-fr-profile
analysis profile AMP_UNIFIED_1-fa-profile
tls-decryption profile TLS_UNIFIED_1-tls-profile
categories never-decrypt
financial-services
log level error
reputation
decrypt-threshold low-risk
sourcedb fail decrypt
policy AIP_1
file-inspection profile AMP_UNIFIED_1-fi-profile
tls-decryption profile TLS_UNIFIED_1-tls-profile
tls-decryption action decrypt
threat-inspection profile IPS_UNIFIED_1
web-filter url profile URLF_UNIFIED_1
```

Wireless Management on Cisco 1000 Series Integrated Services Routers

Radio Profile Definition

```
radio-profile 24ghz
 channel auto
 channel-bandwidth auto

radio-profile 5ghz
 channel auto
 channel-bandwidth auto
```

WLAN Profile Definition

```
wlan-profile TEST-Enterprise
 radio-band all
 vlan-id 300
 ssid TEST-Enterprise
 data-security enterprise
 aaa radius-server 192.168.100.20 auth-port 1812 shared-secret 6
XEJ_TKR[gATN^EOAJfVKBTdcIAeEFHBC^
 qos-type silver

wlan-profile TEST-Personal
 radio-band all
 ssid TEST-Personal
 data-security personal
 passphrase 6 EJcWJK]F_aNQUZBdCDW[aJOKRAHdELKOY
 qos-type silver
```

General Wireless LAN Settings

```
wireless-lan mgmt ip address 192.168.1.11 255.255.255.0 default-gateway 192.168.1.1
 wireless-lan mgmt credential username admin password 6
IPSWCKabbF_OHgaVHZADPAg]UiWLcK]Q^IZKBVS
 wireless-lan country US
```

Qualified Commands for Cisco IOS XE Release 17.6.4

Table 123: Feature History

Feature Name	Release Information	Description
Qualified Configurations for Cisco IOS XE Release 17.6.4	Cisco IOS XE Release 17.6.4	Additional commands are qualified for use in Cisco vManage CLI templates.

Network Address Translation (NAT) Commands

```
ip nat log translations flow-export v9 udp destination IPv4address-port source interface-name
 interface-number
```

Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.7.1a

Table 124: Feature History

Feature Name	Release Information	Description
Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	Additional commands are qualified for use in Cisco vManage CLI templates.

Cisco Unified Border Element Commands

```
address-hiding
anat
```

```
answer-address
application (global)
asserted id
asymmetric payload
audio forced
authentication
bind
block
call spike
call threshold global
call treatment action
call treatment cause-code
call treatment isdn-reject
call treatment on
callmonitor
call-route
clid
codec preference
codec profile
codec transparent
connection-reuse
contact-passing
cpa
credentials
crypto signaling
dial-peer cor custom
dial-peer cor list
dspfarm profile
dtmf-interworking
early-media update block263
early-offer
emergency
error-code-override
error-passthru
g729-annexb override
gcid
header-passing
host-registrar
http client connection idle timeout
http client connection persistent
http client connection timeout
ip qos dscp
localhost
max-conn
media
media-address voice-vrf
media disable-detailed-stats
media-inactivity-criteria
media profile asp
media profile nr
media profile stream-service
media profile video
media-renegotiate
midcall-signaling
min-se
notify redirect
num-exp
options-ping
outbound-proxy
pass-thru content
privacy
privacy-policy
progress_ind
protocol mode
```

```
reason-header override
redirect ip2ip
redirection
referto-passing
registrar
rel1xx
remote-party-id
requri-passing
retry bye
rtcp all-pass-through
rtcp keepalive
rtp payload-type
rtp-media-loop count
rtp-port
rtp-ssrc multiplex
session refresh
session transport
set pstn-cause.
set sip-status
signaling forward
silent discard untrusted
sip-server
srtp
stun
stun usage firewall-traversal flowdata
supplementary-service
timers
transport
uc secure-wsapi
uc wsapi
update-callerid
url (SIP)
vad
voice cause code
voice class codec
voice class dpg
voice class e164-pattern-map
voice class media
voice class server-group
voice-class sip options-keepalive
voice class sip-copylist
voice class sip-event-list
voice class sip-hdr-passthrulist
voice class sip-profiles
voice class srtp-crypto
voice class uri
voice iec syslog
voice statistics iec
```

Cloud onRamp SaaS Commands

```
probe saas-app webex
```

Crypto Commands

```
crypto pki import
```

Dual Endpoint DIA Tracker Commands

```
system
endpoint-tracker tracker-name
    endpoint-dns-name dns-name
```

```
endpoint-ip ip-address
endpoint-api-url api-url
interval seconds
multiplier number
threshold milliseconds
  endpoint-tracker <group-name>  boolean or|and
    tracker-elements <tracker1-name> <tracker2-name>
    tracker-type tracker-group
  interface interface-name
    ip nat outside
        endpoint-tracker  <tracker-group-name>
endpoint-ip <ipv4 address> tcp|udp <port number>
```

Event Commands

```
event ipsla
event manager applet
event manager session cli username
event none
event routing
event syslog
event timer
event track
```

HSRP Commands

```
standby authentication
standby follow
standby ip
standby ipv6
standby mac-address
standby mac-refresh
standby name
standby preempt
standby priority
standby timers
standby track
standby version
show standby
show standby neighbors
```

IP Commands

```
DHCPv6
address prefix
ipv6 address dhcp client request
ipv6 dhcp relay destination
ipv6 dhcp-relay option vpn
ipv6 dhcp client pd
ipv6 dhcp pool
ipv6 dhcp server
ipv6 address autoconfig
prefix-delegation
prefix-delegation pool
vendor-specific
```

Packet Capture Commands

```
monitor capture match ipv4
```

NAT Commands

```
nat66 outside
nat66 prefix
nat66 nd enable
nat66 max-vpn
nat66 route


show commands:
show nat66 prefix
show nat66 statistics
show nat66 dia route
show platform hardware qfp active feature nat66 datapath prefix
show platform hardware qfp active feature nat66 datapath statistics
show platform software nat66 fp active prefix-translation
show platform software nat66 rp active prefix-translation
clear platform hardware qfp active feature nat66 datapath stat
```

Routing Information Protocol Commands

```
address-family ipv4 vrf
auto-summary (RIP)
default-information originate (RIP)
default-metric (RIP)
distance (IP)
distribute-list (RIP)
input-queue
ip rip advertise
ip rip receive version
ip rip send version
maximum-paths
neighbor (RIP)
network (RIP)
offset-list (RIP)
omp-route-tag
output-delay
passive-interface
redistribute
router rip
timers basic (RIP)
traffic-share min
validate-update-source
version (RIP)
show ip protocols
show ip rip database
show ip rip neighbors
show ip route vrf
```

SNMP Commands

```
snmp-server enable traps config-copy
snmp-server enable traps config-ctid
snmp-server enable traps cpu
snmp-server enable traps event-manager
snmp-server enable traps flash
snmp-server enable traps memory
snmp-server enable traps syslog
snmp-server sparse-tables
snmp trap link-status
```

System Commands

```
gps-location (system)
```

Tracker Commands

```
boolean
endpoint-api-url
endpoint-dns-name
endpoint-ip
endpoint-tracker
interval
multiplier
threshold
tracker-elements
tracker-type
tracker-type
show endpoint-tracker
show ip sla summary
```

Unified Logging for Security Connection Events

```
ZBFW
Use this configuration to enable Unified Logging for ZBFW at a global level.
Device(config)# parameter-map type inspect-global
Device(config-profile)# log flow

UTD
Use this configuration to enable Unified Logging for all UTD features.
Device(config)# utd engine standard unified-policy
Device(config-utd-unified-policy)# utd global
Device(config-utd-mt-global)# flow-logging all
Device(config-utd-mt-global)# flow-logging all {file-inspection threat-inspection
web-filtering}

Configure Netflow
Use this configuration to enable Netflow to export log data of ZBFW and UTD features to an
 external collector
Device(config)# flow exporter exporter-name
Device(config-flow-exporter)# description description
Device(config-flow-exporter)# destination IP address
Device(config-flow-exporter)# export-protocol netflow-v9
Device(config-flow-exporter)# transport udp udp-port

show performance monitor context temp0 configuration
show performance monitor context temp1 exporter
show performance monitor context temp1 traffic-monitor sdwan-fnf-vpn0-stats cache
```

VRRP Commands

```
object (tracking)
track interface
track list
track service
tloc-change increase-preference
vrrp address-family
vrf forwarding
show vrrp
```

Troubleshooting Commands

```
monitor capture match ipv4
show autoip status
show crypto key mypubkey rsa
```

```
show crypto pki certificates
show crypto session
show endpoint-tracker
show flow monitor sdwan_flow_monitor cache
show ip protocols
show ip rip database
show ip rip neighbors
show ip route rip
show ip route vrf
show ip sla summary
show ipv6 dhcp binding
show ipv6 dhcp database
show ipv6 dhcp interface
show ipv6 dhcp pool
show platform hardware qfp active classification class-group-manager class-group client cce
 name
show platform hardware qfp active feature firewall drop
show platform hardware qfp active feature nat66 datapath prefix
show platform hardware qfp active feature nat66 datapath statistics
show platform software nat66 fp active
show platform software nat66 rp active
show policy-firewall config
show policy-map type inspect
show nat66 dia route
show nat66 nd
show nat66 prefix
show nat66 statistics
show sdwan bfd sessions region-access
show sdwan bfd sessions region-core
show sdwan cloudexpress applications
show sdwan omp cloudexpress
show sdwan omp peers
show standby
show standby neighbors
show track
show vrrp
```

Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.8.1a

Table 125: Feature History

Feature Name	Release Information	Description
Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	Additional commands are qualified for use in Cisco vManage CLI templates.

Access Point Name (APN) Commands

```
profile id <id> apn <name> authentication <type> pdn-type <type>
```

Cloud onRamp for SaaS Commands

```
probe saas-app <applist name>
app <app1>
```

```
app <app2>
endpoint-fqdn   DNS name of saas-app endpoint
endpoint-ip     IP address of saas-app endpoint
endpoint-url    API url of saas-app endpoint
```

Hierarchical SD-WAN Commands

```
region <region_id> [secondary-region <region_id>]
region (secondary-shared | secondary-only)
omp best-path region-path-length ignore
transport-gateway enable
omp best-path transport-gateway [prefer | ecmp-with-direct-path]
match route transport-gateway-reoriginated
affinity-group <number>
affinity-group-preference <number1> <number2> …
filter route outbound affinity-group preference
```

IP Commands

```
ip cef load-sharing algorithm src-only [id]
ipv6 cef load-sharing algorithm src-only
ip load-sharing algorithm src-ip-only
ipv6 load-sharing algorithm src-ip-only
```

Network Address Translation (NAT) Commands

```
ip nat inside source static 10.0.0.1 12.0.0.1 vrf 1 match-in-vrf track  <track-id>
ip nat inside source list global-list pool natpool2 vrf 1 match-in-vrf overload track
<track-id>
```

Routing Information Protocol Next Gen (RIPng) Commands

```
ipv6 rip vrf-mode enable
ipv6 rip enable
ipv6 router rip sdwan
address-family ipv6 vrf <vpn-id>
omp-route-tag
distribute-list prefix-list <ipv6-prefix-list-name> {in | out}
redistribute {omp | static | connected | ospf <id>} [route-map <route-map-name>] [metric
<1-15>]
ipv6 rip default-information {only | originate} [metric <1-15>]
ipv6 rip metric-offset <value>
ipv6 rip summary-address <ipv6-add>
```

Voice Commands

```
caller-id alerting dsp-pre-allocate
caller-id alerting line-reversal
caller-id alerting pre-ring
caller-id alerting ring [ 1 | 2 | 3 | 4 ]
caller-id block
caller-id format 911
caller-id mode {BT | FSK | DTMF [start | end {# | * | A | B | C | D}]}
clid dtmf-codes <start-code><redirect-code><end-code>
```

Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.9.1a

Table 126: Feature History

Feature Name	Release Information	Description
Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	Additional commands are qualified for use in Cisco vManage CLI templates.

AppQoE Commands

```
sdwan appqoe tcptopt http-connect port port-number
```

Cisco SD-WAN Identity-Based Firewall Policy Commands

```
identity
  pxgrid
    server-address name>
    username name>
    password name>
    subscriptions {user-identity | sgt}
    domain-name domain-name>
    vpn 0

class-map type inspect match-any cm3
    match identity user-group source Engineering
    match identity user-group source Security
    match identity user source Jim

class-map type inspect match-all cm4
    match access-group name group-name>
    match application-class>
    match protocol-class>
    match identity-class-cm3>

policy-map type inspect pm1
    class type inspect cm4
         inspect
```

Network Address Translation (NAT) Commands

```
ip nat service all-algs
ip nat service dns tcp
ip nat service dns udp
ip nat service ftp
ip nat service sip tcp port port-number
ip nat service sip udp port port-number


ip nat inside source static tcp ip-address port ip-address port egress-interface
interface-type-number
ip nat inside source static tcp ip-address port interface interface-type-number

ip nat outside source static ip-address ip-address vrf vrf-name redundancy
```

```
hsrp-standby-group-name match-in-vrf

ip nat log translations flow-export v9 udp destination IPv4address-port source interface-name
 interface-number
```

Policy Configuration Tagging Commands

```
tag-instances [tag-instance] [lists]

tag-instance tag-instance-name [id global-unique-id][app-list app-list-name] [data-prefix-list
 prefix-list-name] [data-ipv6-prefix-list ipv6-prefix-list-name]

lists [app-list app-list-name] [data-prefix-list prefix-list-name] [data-ipv6-prefix-list
ipv6-prefix-list-name]

match [destination-tag-instance dest-tag-name | source-tag-instance src-tag-name]

match [destination-tag-instance dest-tag-name | source-tag-instance  src-tag-name |
tag-instance  tag-name]

match[destination-tag-instance dest-tag-name | source-tag-instance src-tag-name | tag-instance
  tag-name]

access-list acl-name sequence sequence-number match source-tag-instance src-tag-name

access-list acl-name sequence sequence-number match destination-tag-instance dest-tag-name
```

Route Leaking Between Service VPNs

```
route-replicate from vrf source-vrf-name unicast protocol [route-map map-tag]

redistribute vrf vrf-name protocol subnets [route-map map-tag]
```

Qualified Commands for Cisco IOS XE Release 17.10.1a

Table 127: Feature History

Feature Name	Release Information	Description
Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	Additional commands are qualified for use in Cisco vManage CLI templates.

AAA Commands

```
no ip scp server enable
no ip http tls-version TLSv1.1
no ip http tls-version TLSv1.0
ip http tls-version TLSv1.2
no snmp-server system-shutdown
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
aaa group server tacacs+ tacacs-100
tacacs server <server name>
port <xx> timeout <xx>
aaa accounting connection default start-stop group
aaa authorization credential-download [default | <string>] <group-name>
```

Cisco SD-WAN Identity-Based Firewall Policy Commands

```
identity
  pxgrid
    server-address name>
    username name>
    password name>
    subscriptions {user-identity | sgt}
    domain-name domain-name>
    vpn 0
class-map type inspect match-any cm3
    match identity user-group source Engineering
    match identity user-group source Security
    match identity user source Jim
class-map type inspect match-all cm4
    match access-group name group-name>
    match application-class>
    match protocol-class>
    match identity-class-cm3>
object-group security sec-source
    security-group tag 100
    security-group tag 200
    security-group tag 300
object-group security sec-dest
    security-group tag 400
    security-group tag 500
policy-map type inspect pm1
    class type inspect cm4
         inspect
```

CUBE Commands

```
conn-reuse
disable-early-media 180
gw-accounting
handle-replaces
max-forwards
nat
notify ignore substate
notify telephone-event
permit hostname
random-contact
retry invite
srtp negotiate
stun flowdata shared-secret
video codec
voice class codec preference
voice class tls-cipher
voice class tls-profile
xfer target

credentials
security-policy (voice register global)
translation-profile (voice register)
```

DHCP Commands

```
ip dhcp client vendor-class
ipv6 dhcp client vendor-class
```

Network Address Translation (NAT) Commands

```
ip nat settings preserve-sdwan-ports
nat64 route
nat64 settings
nat64 settings mtu (mtu keyword added for 17.10.1.a)
nat64 provisioning
```

Security Command

```
threat-inspection custom-signature profile
```

System Commands

```
system
gps-location latitude 32.0
gps-location longitude -100.0
system-ip 172.16.255.14
domain-id 1
site-id 400
ipv6-strict-control true
admin-tech-on-failure
organization-name "vIPtela Inc Regression"
vbond vbond
!
```

Underlay Measurement and Tracing Services Commands

```
sdwan
umts
monitor
periodicity 30
local-color-all
remote-color-all
remote-system-ip-all
!
event
event-type tunnel-sla-change
local-color-all
remote-color-all
remote-system-ip-all
!
event-type tunnel-pmtu-change
local-color-all
remote-color-all
remote-system-ip-all
!
```

Qualified Commands for Cisco IOS XE Release 17.11.1a

Table 128: Feature History

Feature Name	Release Information	Description
Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	Additional commands are qualified for use in Cisco vManage CLI templates.

IP Commands

```
ntp disable ip/ipv6
radius server <server-name>
ipv6 nd autoconfig default-route
aaa group server tacacs+
ip tacacs source-interface
server-private (TACACS+)
tacacs server address ipv4
aaa group server radius
ip radius source-interface
ipv6 tcp adjust-mss
ipv6 radius source-interface
ipv6 address dhcp
ipv6 tacacs source-interface
ipv6 address dhcp client request
ipv6 access-class
ipv6 address autoconfig
ipv6 dhcp client pd
ipv6 enable
ntp access-group
ntp server


object-group v6-network ipv6-og1 host 2001:DB8:1::1 2002::1/64
object-group v6-network ipv6-og2 host 2001:DB8:2::1 2003::1/64
ipv6 access-list ipv6acl permit ipv6 ::2 2001:3c0:1::64/128
ipv6 access-list ipv6-acl2
permit tcp object-group ipv6-og1 object-group ipv6-og2
class-map type inspect match-any ipv6cm
match access-group name ipv6acl
match access-group name ipv6acl2
policy-map type inspect ipv6pm

 class type inspect ipv6cm
inspect
zone security inside
  vpn 1
zone security outside
   vpn 0
zone-pair security zp source-zone inside destination-zone outside
service-policy type inspect ipv6pm

Firewall Support for Dual Stack of IPv4 and IPv6

object-group network ipv4-og1
host 192.168.12.10 host 192.168.12.11
object-group network ipv4-og2 host 192.168.12.12
host 192.168.12.13
object-group v6-network ipv6-og1
host 2001:DB8:1::1 2002::1/64
object-group v6-network ipv6-og2
host 2001:DB8:2::1 2003::1/64

ip access-list extended ipv4acl
permit tcp 0.0.0.2 255.255.255.0 0.0.0.3 255.255.255.0
ipv6 access-list ipv6acl
permit ipv6 ::2 ::3
ip access-list extended ipv4-acl2
permit udp object-group ipv4-og1 object-group ipv4-og2
ipv6 access-list ipv6-acl2
permit tcp object-group ipv6-og1 object-group ipv6-og2
class-map type inspect match-any dualcm

 match access-group name ipv4acl
```

```
 match access-group name ipv6acl

 match access-group name ipv4-acl2

 match access-group name ipv6-acl2
policy-map type inspect dualpm

 class type inspect dualcm
  inspect
zone security inside
   vpn 1
zone security outside
   vpn 0
zone-pair security zp source-zone inside destination-zone outside

 service-policy type inspect dualpm
```

Multicast Commands

```
multicast
 address-family ipv4 vrf 1
 replicator
 spt-only
 msdp-interworking
```

Multi-Region Fabric Commands

```
advertise aggregate prefix <pfx> … [region <access | core>]

system
 host-name             vm9
 gps-location latitude 45.0
 gps-location longitude -122.0
 system-ip             172.16.255.19
 site-id               100
 tloc-color-compatibility
  compatible lte private1
  !
  compatible private1 private2
  !
  incompatible lte default
  !
  incompatible lte 3g
  !
 !

omp
  no shutdown
  ecmp-limit       6
  graceful-restart
  no as-dot-notation
  timers
   holdtime                       15
   tloc-color-cap-update-interval 120
   graceful-restart-timer         120
  exit

show running-config policy
policy
 control-policy test-affinity
  sequence 1
```

```
   match route
    site-id 100
   !
   action accept
    set
     affinity-group-number 2
    !
   !
  !
  sequence 2
   match tloc
    tloc 172.16.255.21 color lte encap ipsec
   !
   action accept
    set
     affinity-group-number 5
    !
   !
  !
  default-action reject
 !
!
```

NAT Commands

```
ip nat service all-algs
ip nat service H225
ip nat service ras
ip nat service pptp
ip nat service tftp
ip nat service sunrpc tcp
ip nat service sunrpc udp


ip nat inside source static tcp 10.0.0.12 8080
interface Loopback15 8585 vrf 1 egress-interface GigabitEthernet3
```

Policy Commands

```
Device(config)# policy log-rate-limit

(<1..10000> logs per second. Default is 25) (25):



Device# show sdwan running-config policy
policy
no app-visibility
no app-visibility-ipv6
no flow-visibility
no flow-visibility-ipv6
no implicit-acl-logging
log-frequency        1000
log-rate-limit    25
access-list ACL1
  sequence 1
   match
    dscp 10
   !
   action accept
    count CNT2
    log
   !
  !
```

```
  default-action drop
!
!
```

Tunnel Interface Commands

```
gre-in-udp


match-inner ipv4
match-inner ipv6
mpls match-inner ipv4
allow-no-label
mpls match-inner ipv6
mpls <label> <depth> match-inner ipv4
mpls <label> <depth> match-inner ipv6
```

Zone Based Firewall Commands

```
parameter-map type inspect-global
log flow-export v9 udp destination 10.10.10.50 5050 source interface GigabitEthernet0/0/5
log flow-export v9 udp destination 10.10.10.51 5050 source interface GigabitEthernet0/0/5
log flow-export v9 udp destination 10.10.10.52 5050 source interface GigabitEthernet0/0/5
log flow-export v9 udp destination 10.10.10.53 5050 source interface GigabitEthernet0/0/5


logging host 10.10.10.1 source-interface Loopback10
```

Qualified Commands for Cisco IOS XE Release 17.12.1a

Table 129: Feature History

Feature Name	Release Information	Description
Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	Additional commands are qualified for use in Cisco SD-WAN Manager CLI templates.

AAA Commands

```
 aaa
lockout-policy
fail-attempts 3 fail-interval 300 lockout-interval 100
num-inactive-days days
multi-factor-auth
duo
api-hostname name
secret-key s-key
integration-key i-key
proxy proxy-url
```

Hub and Spoke Commands

```
topology hub-and-spoke enable
```

IP Commands

```
ip virtual-reassembly
```

MACsec Commands

```
key chain mac_chain macsec
key 1234abcd5678
key-string 12345678123456781234567812345678 cryptographic-algorithm AES-128-CMAC
key-string 11111111111111111111111111111111 cryptographic-algorithm aes-256-cmac
lifetime 05:00:00 20 february 2015 12:00:00 30 september 2016
mka policy MKAPolicy
confidentiality-offset
key-server priority 1
delay-protection
mka policy 2
include-icv-indicator
macsec-cipher-suite gcm-aes-256
sak-rekey interval 300
use-updated-eth-header
mka pre-shared-key key-chain kc1
macsec access-control must-secure
macsec access-control should-secure
macsec replay-protection window-size 10
eapol eth-type 0xB860
eapol destination-address 0018.b967.3cd0
eapol destination-address bridge-group-address
eapol destination-address broadcast-address
eapol destination-address lldp-multicast-address
cryptographic-algorithm aes-128-cmac
macsec-cipher-suite gcm-aes-128
macsec-cipher-suite gcm-aes-256
macsec-cipher-suite gcm-aes-xpn-128
macsec-cipher-suite gcm-aes-xpn-256
send-secure-announcements
macsec disable-sci
macsec replay-protection window-size 1024
macsec dot1q-in-clear
```

NAT Commands

```
nat66 prefix inside 2001:DB8::/32 outside 2001:DB8::/48 vrf 1 egress-interface GigabitEthernet
 3

nat66 prefix inside 2001:DB8::/32 outside 2001:DB8::/48 egress-interface GigabitEthernet 3
```

Routing Commands

```
affinity-group preference-auto
affinity-per-vrf
redistribute omp translate-rib-metric
```

Transport Gateway Commands

```
site-type
```

Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.13.1a

Table 130: Feature History

Feature Name	Release Information	Description
Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.13.1a	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a	Additional commands are qualified for use in Cisco SD-WAN Manager CLI templates.

Interface Commands

```
  interface  GigabitEthernet  slot/subslot/port
 no ip address
 channel-group  channel-group-number  mode { active  passive}
 exit
lacp  system-priority  priority
 interface  GigabitEthernet  slot/subslot/port
 lacp  port-priority  priority
config-transaction
 interface  GigabitEthernet  slot/subslot/port
 no ip address
 channel-group  channel-group-number
```

IP Commands

```
ip dhcp smart-relay
```

Multi-Region Fabric Commands

```
management-gateway
management-region
```

NAT Commands

```
nat66 prefix inside source-prefix outside interface interface-name

nat66 prefix inside source-prefix outside interface interface-name vrf 1
```

SD-WAN Tunnel Interface Commands

```
interface  Tunnel  tunnel-number
 ip unnumbered  Port-channel channel-group-number
 no ip redirects
 tunnel source   Port-channel channel-group-number
 tunnel mode sdwan
 interface  Port-channel  channel-group-number
 tunnel-interface
 encapsulation { ipsec gre}
 color { public-internet mpls biz-internet lte}
```

Tracker Commands

```
tracker-type interface-icmp

tracker-type ipv6-interface-icmp

icmp-interval

endpoint-tracker-settings dia-stabilize-status
```

Service Insertion Commands

```
service-chain
service-chain-affect-bfd
service-chain-description
service-chain-enable
service-chain-vrf
service-track-enable
```

Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.14.1a

Table 131: Feature History

Feature Name	Release Information	Description
Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.14.1a	Cisco IOS XE Catalyst SD-WAN Release 17.14.1a	Additional commands are qualified for use in Cisco SD-WAN Manager CLI templates.

Interface Commands

```
port-channel load-balance-hash-algo sdwan
ip load-sharing algorithm src-dst-ip


port-channel load-balance-hash-algo sdwan
ipv6 load-sharing algorithm ip-and-ports
```

L2VPN Commands

```
l2vpn sdwan instance 10 point-to-point
l2vpn sdwan instance 11 multipoint

interface GigabitEthernet7
 service instance 20 ethernet
  encapsulation dot1q 200
  !
 service instance 21 ethernet
  encapsulation dot1q 201
  !
bridge-domain 30
 member GigabitEthernet7 service-instance 20
 member sdwan-instance 10  remote-site 2 vc-id 1 single-homing
```

```
bridge-domain 31
 member GigabitEthernet7 service-instance 21
 member sdwan-instance 11 vc-id 1 single-homing
```

NAT Commands

```
nat66 prefix inside source-prefix outside interface interface-name

nat66 prefix inside source-prefix outside interface interface-name vrf 1
```

Policy Commands

```
policy app-agg-node max-records-per-minute
```

Tracker Commands

```
endpoint-tracker-sla-profile sla_agg
loss 10
latency 300
jitter 80
sla-mode aggressive
```

Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.15.1a

Table 132: Feature History

Feature Name	Release Information	Description
Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.15.1a	Cisco IOS XE Catalyst SD-WAN Release 17.15.1a	Additional commands are qualified for use in Cisco SD-WAN Manager CLI templates.

Cellular Commands

```
controller cellular 0/1/0
lte gps constellation gps
```

High Availability Commands

```
redundancy
application redundancy
preempt
init-role standby
init-role active
path-optimization
redundancy rii 350
```

L2VPN Commands

```
bridge-domain 10
  member GigabitEthernet7 service-instance 20
```

```
  member sdwan-instance 10  remote-site 2 vc-id 1 dual-homing
exit
bridge-domain 20
  member GigabitEthernet7 service-instance 21
  member sdwan-instance 11 vc-id 1 dual-homing
```

Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.16.1a

Table 133: Feature History

Feature Name	Release Information	Description
Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.16.1a	Cisco IOS XE Catalyst SD-WAN Release 17.16.1a	Additional commands are qualified for use in Cisco SD-WAN Manager CLI templates.

SD-WAN Tunnel Interface Commands

```
sdwan

interface GigabitEthernet1

bandwidth-downstream 300000000
bandwidth-upstream 300000000
```

Cisco Unified Border Element Commands

```
voice class codec
video codec codec-type
codec preference value codec-type
dial peer
rtp payload-type codec-audio-scip payload-type-number
rtp payload-type codec-video-scip payload-type-number
```

Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.18.1a

Table 134: Feature History

Feature Name	Release Information	Description
Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.18.1a	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a	Additional commands are qualified for use in Cisco SD-WAN Manager CLI templates.

Cellular Commands

```
Router(config-controller)#lte modem crash-action
  auto-collect   Remain in crash state and auto collect crash dump
  boot-and-hold  Remain in crash state
Router(config-controller)#lte modem crash-action auto-collect
```

```
CellularGateway# cellular 0/2/0 profile-reset
```

Crypto Commands

```
crypto pki trustpoint TP-self-signed-3865005142
 enrollment selfsigned
crypto pki trustpoint ca-check-strict
```

Ignition Power Management Commands

```
ignition sense-voltage on-threshold 11 900 off-threshold 11 500
```

Line Commands

```
ip telnet disable
```

Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 26.1.1

Table 135: Feature History

Feature Name	Release Information	Description
Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 26.1.1	Cisco IOS XE Catalyst SD-WAN Release 26.1.1	Additional commands are qualified for use in Cisco SD-WAN Manager CLI templates.

Cube Commands

```
cipher (voice class)
```

```
http client secure-ciphersuite
```

```
transport tcp tls
```

Global Configuration Commands

```
Device(config-sdwan)# speedtest disable-backward-compatible-ip
```

System Commands

```
Device(config)# statistics
Device(config-statistics)# table interface
Device(config-table-interface)# collection-interval 1
```